Miša Gleni

DARKMARKET

Kako su hakeri postali nova mafija

S engleskog prevela Tanja Milosavljević

Prolog

crime@21stcentury.com

U svom neumoljivom ljudskom porivu za pogodnostima i ekonomskim razvojem, za vrlo kratko vreme razvili smo opasan nivo zavisnosti od umreženih sistema: za manje od dve decenije, ogromni delovi takozvane „kritične nacionalne infrastrukture" (critical national infrastructure – CNI na jeziku gikova) našli su se u većini zemalja pod kontrolom još složenijih kompjuterskih sistema.

Kompjuteri rukovode velikim delom našeg života, budući da upravljaju našim komunikacijama, vozilima, našim trgovinskim transakcijama i interakcijama s državom, našim poslom, dokolicom, ama baš svime. Na jednom od suđenja za sajber kriminal kojima sam poslednjih godina prisustvovao, britansko državno tužilaštvo zahtevalo je izdavanje rešenja o prevenciji zločina jednom hakeru, koje bi postalo pravosnažno pošto ovaj izađe iz zatvora. Tim rešenjem bi mu pristup internetu bio dozvoljen samo jedan sat nedeljno, i to pod nadzorom policijskog službenika. „Kad moj klijent konačno odsluži zatvorsku kaznu", primetio je na saslušanju advokat optuženog, „jedva da će i postojati neka ljudska aktivnost koja se neće obavljati posredstvom interneta. Pod takvim okolnostima, kako da moj klijent živi iole normalnim životom?", glasilo je retoričko pitanje.

Zaista, kako? Oni koji zaborave mobilni telefon kod kuće, obično već posle nekoliko sati primete kod sebe izrazitu nervozu i osećaj gubitka, koji kod posebno zavisnih korisnika prelaze u stanje slično onome posle naglog skidanja s droge („cold turkey"). Zanimljivo je da se, nakon što su tri dana lišeni pomenute naprave, ovaj izjedajući osećaj nelagode često povlači pred naletom oslobođenosti koja nastupa zajedno s povratkom čoveka u ne tako daleki svet u kome nismo imali mobilni niti nam je bio potreban i uređivali smo sebi život u skladu s tim. Danas većina

ljudi smatra da ne može da živi bez ovih majušnih prenosivih kompjutera.

Možda je najbliže poređenje kompjutera i motornih vozila. Kad su kola, negde četrdesetih godina prošlog veka, postala standardni deo porodičnog domaćinstva, samo je veoma mali broj vozača zaista razumevao šta se odvija ispod poklopca motora. I pored toga, ipak je bilo dosta onih koji su umeli da poprave svoje vozilo bez obzira na uzrok kvara, još više onih koji su umeli da privole karburator da proradi makar toliko da se odvuku do kuće, a većina je umela barem da promeni probušenu gumu.

Ovih dana, ako je posredi samo probušena guma, po svoj prilici ćete ipak stići na odredište. Međutim, sve veći broj današnjih kvarova rezultat je kompjuterske greške u upravljačkoj jedinici motora – kućištu od crne plastike koje se obično nalazi iza samog motora. Ako je problem u upravljačkoj jedinici, tada nema šanse da pokrenete kola čak ni ako ste iskusni tenkovski mehaničar. Ukoliko imate sreće, možda će kompjuterski inženjer uspeti da je popravi. Međutim, u većini slučajeva moraćete da zamenite kompletnu upravljačku jedinicu.

Kompjuterski sistemi su toliko složeniji i krhkiji od motora s unutrašnjim sagorevanjem da samo neverovatno mala grupa ljudi ume uopšte i da počne da se bavi problemom dalje od poznate mantre: „Jesi li probao da ga restartuješ?"

Danas se nalazimo u situaciji u kojoj ova malobrojna elita (nazovimo ih gikovima, tehnomanijacima, hakerima, koderima, sekurokratama ili kako god) izvanredno dobro poznaje tehnologiju koja svakog dana sve jače i u sve većoj meri upravlja našim životom, dok najveći deo nas ostalih o njoj ne zna ama baš ništa. Značaj toga počeo sam da poimam dok sam sakupljao materijal za svoju prvu knjigu o organizovanom kriminalu, *Mekmafija*.[1] U nameri da istražim sajber kriminal, otputovao sam u Brazil, zato što je ova izuzetno zanimljiva zemlja – među mnogim svojim pozitivnim osobinama – glavni centar svega onoga što ne valja na Mreži, mada je to tada bilo malo poznato.

Tamo sam upoznao sajber lopove koji su osmislili spektakularno uspešnu „pecačku" prevaru. Phishing ili pecanje je i dalje jedan od najpouzdanijih oslonaca kriminala na internetu. Postoje dve jednostavne varijante. Žrtva otvori spam imejl. Prilog može sadržavati virus, koji omogućava kompjuteru na nekom drugom

1 Srpsko izdanje: Samizdat B92, Beograd, 2008.

mestu u svetu da prati sve aktivnosti zaraženog kompjutera, uključujući i unos bankovnih lozinki. Drugi trik sastoji se u osmišljavanju imejla koji izgleda kao da ga je poslala banka ili neka druga ustanova, kojim se zahteva potvrda podataka i lozinke unesenih prilikom logovanja. Ukoliko primalac nasedne na smicalicu, spamer ih može upotrebiti za pristup nekim ili svim vašim internet računima. Brazilski hakeri demonstrirali su, korak po korak, kako su sebi obezbedili desetine miliona dolara s bankovnih računa u Brazilu, Španiji, Portugalu, Ujedinjenom Kraljevstvu i Sjedinjenim Državama.

Potom sam posetio sajber policajce u Braziliji koji su uhapsili četiri pripadnika te kriminalne grupe (premda ih je ostalo najmanje dvostruko više kojima policija nikad nije ušla u trag), a onda sam intervjuisao starešinu Iks-jedinice (X-Force), odeljenja za tajne operacije pri američkoj kompaniji ISS, koja se bavi kompjuterskom bezbednošću. Za ciglo nedelju dana, shvatio sam da konvencionalni ili tradicionalni organizovani kriminal, sve onako živopisan i raznorodan kakav jeste, nosi sa sobom znatno veće rizike za počinioce u odnosu na one umešane u sajber kriminal.

Ako hoće da budu uspešne u zanimanju koje su odabrale, staromodne grupe za organizovani kriminal, koje se drže tehnologije i sredstava iz XX veka, moraju da prevaziđu dve zastrašujuće prepreke. Njihov primarni poslovni rizik predstavlja policija. Efikasnost kriminalističkih službi varira i geografski i s vremenom. Grupe za organizovani kriminal se prilagođavaju tim promenljivim okolnostima i biraju jednu od brojnih metoda za izlaženje na kraj sa snagama reda i zakona. Pokušavaju da ih nadjačaju golom silom; podmićuju ih; podmićuju političare koji imaju uticaj na policiju; ili nastoje da izbegnu da im one uđu u trag.

Potom se suočavaju s drugim problemom: s pretnjama konkurencije, ostalih loših momaka koji krstare istim vodama u potrazi za plenom. I tu mogu pokušati da pobede golom silom; mogu predložiti formiranje savezništva; ili mogu pristati da ih ovi progutaju.

Ni u jednom slučaju, međutim, sindikat zločina ih ne može naprosto ignorisati – to je recept za neuspeh, katkada s kobnim rezultatima. Ključ opstanka i prosperiteta jeste sposobnost da komunicirate s kolegama kriminalcima i policijom – i, štaviše, da obema grupama šaljete ispravne poruke.

U Brazilu sam vrlo brzo shvatio da je kriminal XXI veka drugačiji.

Što je najvažnije, na Mreži je mnogo, mnogo teže odrediti kad vam neko ne misli dobro. Zakoni koji se odnose na internet veoma se razlikuju od države do države. To je bitno zato što će se, generalno, krivično delo preko Mreže izvršiti sa IP (internet protokol) adrese u jednoj zemlji, a na štetu fizičkog ili poslovnog lica u drugoj zemlji, da bi se potom realizacija (ili isplata) odigrala u nekoj trećoj državi. Možda, na primer, policajcu u Kolumbiji uspe da ustanovi da se IP adresa koja koordinira napad na kolumbijsku banku nalazi u Kazahstanu. Međutim, potom saznaje da se u Kazahstanu to ne smatra krivičnim delom, zbog čega njegov kolega u tamošnjem glavnom gradu nema razloga da istražuje taj zločin.

Mnogi sajber kriminalci su dovoljno inteligentni da istraže i iskoriste takve neusaglašenosti. „Nikad ne koristim američke kreditne ili debitne kartice", rekao mi je jedan od najuspešnijih švedskih „kartičara", „zato što bih tako, gde god da se nalazim na planeti, dospeo pod pravnu jurisdikciju Sjedinjenih Država. Stoga radim samo evropske i kanadske kartice, što me potpuno zadovoljava i garantuje mi bezbednost – nikad me neće uhvatiti."

Granica koja razdvaja Sjedinjene Države od Evrope i Kanade je izuzetno važna, budući da su to oblasti u kojima živi najveća koncentracija žrtava sajber kriminala. Ove potonje teritorije imaju mnogo jače zakone koji štite slobode i prava pojedinca na Mreži. Američke vlade redovno daju kriminalističkim službama veća ovlašćenja od onih koja bi većina evropskih vlada i pomislila da im dâ, omogućavajući policiji, u ime borbe protiv kriminala i terorizma, lakši pristup podacima iz privatnih kompanija.

Implikacije ovoga su istovremeno duboke i, barem zasad, nepojmljive. Sporna pitanja u vezi sa kriminalom, nadzorom, privatnošću, prikupljanjem podataka od privatnih i državnih institucija, slobode govora (istupi, Vikilikse), lakoćom pristupa vebsajtovima (takozvana debata o neutralnosti neta), prisustvom na društvenim mrežama kao sredstvom u političkoj borbi i interesima nacionalne bezbednosti neprestano se sudaraju u sajber prostoru.

Neko će reći, na primer, da multiplatformska, multiprogramska sveprisutnost Googlea krši principe antimonopolskih zakona Amerike, te da gomilanje svih tih ličnih podataka istovremeno predstavlja priliku za kriminalce i pretnju građanskim slobodama. Google

pak može na to odgovoriti da suština njegovog genija i uspeha leži upravo u njegovoj multiplatformskoj i multiprogramskoj sveprisutnosti, te da to samo po sebi ide u korist komercijalnim i bezbednosnim interesima Amerike. Ako poželi, vlada SAD može primeniti pravne postupke i za samo nekoliko sati dobiti pristup podacima u posedu Googlea, a budući da Google prikuplja podatke iz celog sveta, to Vašingtonu daje ogromnu stratešku prednost. Ostale vlade nisu te sreće. Za razliku od svojih kineskih, ruskih ili bliskoistočnih kolega, američka vlada ne mora da hakuje Google kako bi istražila njegove tajne. Umesto toga, može da pribavi sudski nalog. Da li biste se zaista odrekli toga u ime doslednog sprovođenja antimonopolskih zakona?

Internet je poput teorije o velikom mehuru – rešite jedan problem koji mu smeta, ali onda negde drugde iskrsne drugi, naizgled nerešiv.

Za kriminalističke službe pak najveći problem jeste anonimnost. Kako sada stvari stoje, svakome ko ima pristup internetu, a poseduje neophodno i lako dostupno znanje, savršeno je moguće da maskira fizičku lokaciju kompjutera.

To se može uraditi na dva osnovna načina – prvi sajber zid je VPN ili Virtual Private Network (virtualna privatna mreža), u kojoj grupa kompjutera može da deli jednu te istu IP adresu. Ta IP adresa obično se odnosi na jedan uređaj, ali uz pomoć VPN-a postiže se privid da je nekoliko kompjutera, koji se zapravo nalaze na više mesta u svetu, smešteno, na primer, u Bocvani.

Oni koji se ne zadovoljavaju zaštitom koju pruža VPN mogu podići još jedan sajber zid, i to upotrebom takozvanih proksi servera. Kompjuter smešten na Sejšelima može koristiti proksi u, recimo, Kini ili Gvatemali. Proksi ne otkriva da se originalni IP emituje sa Sejšela, a i taj kompjuter je, opet, deo VPN-a s bazom na Grenlandu.

Organizovanje svega ovoga zaista zahteva posedovanje naprednog poznavanja kompjutera, zbog čega ove tehnike najčešće koriste dve grupe koje se bave sajber kriminalom – pravi hakeri i pravi kriminalci. Međutim, ti sofisticirani stručnjaci koji predstavljaju novi vid ozbiljno organizovanog kriminala čine tek manjinu umešanih u kompjuterski kriminal.

Ostalo su sitni igrači koji rade samostalno i s relativno trivijalnim sumama novca, u suštini, sitni lopovi koje se jedva i isplati loviti s obzirom na oskudne resurse koji stoje na raspolaganju

kriminalističkim službama. Mada se ti likovi ne gnjave podizanjem VPN-a, proksija i kojekakvim drugim tehnikama maskiranja, šifrovanom komunikacijom ipak umeju da značajno zagorčaju život policajcima.

Softver koji garantuje enkripciju vaše pismene (pa čak i audio i video) komunikacije besplatan je i široko dostupan na Mreži; najviše se koristi PGP, akronim za veseli kolokvijalni naziv koji glasi Pretty Good Privacy (otprilike: „prilično uspešna privatnost").

Enkripcija ili šifrovanje je moćna alatka koja igra važnu ulogu u sajber bezbednosti. To je vid brkanja jezika uz pomoć digitalno generisanih ključeva, čije su permutacije matematički toliko astronomske da se mogu otkriti samo ako znate šifru. Zasad su šifrovani dokumenti zaista sigurni, mada vašingtonska Agencija za nacionalnu bezbednost (National Security Agency, NSA), najmoćnija digitalna špijunska agencija na svetu, povazdan radi na tome da ih provali. U bratstvu sajber kriminala već uveliko kolaju glasine da NSA i njeni partneri u biznisu sakupljanja informacija u Kanadi, Britaniji, Australiji i Novom Zelandu poseduju sposobnost da provale ove javne sisteme za enkripciju pomoću svog orvelovskog sistema nazvanog Echelon. Kako se u izveštajima navodi, Echelon može da pristupi telefonskim, imejl i satelitskim komunikacijama bilo gde u svetu.

Političke implikacije digitalne enkripcije tako su ogromne da je vlada Sjedinjenih Država 1990-ih počela da klasifikuje softver za enkcipciju kao „tešku artiljeriju", dok vam u Rusiji, ako policija ili KGB pronađu jedan jedini šifrovani fajl u vašem kompjuteru, preti višegodišnja zatvorska kazna, pa makar dokument sadržavao samo vašu nedeljnu listu za kupovinu. Kako vlade i korporacije prikupljaju sve više ličnih podataka o svojim građanima ili klijentima, enkripcija je jedna od malobrojnih mogućnosti odbrane preostalih pojedincima kako bi zaštitili svoju privatnost. Ujedno je i dragocen instrument za one koji su umešani u kriminalne radnje na Mreži.

Baš kao što tradicionalni kriminalci moraju da razviju specifične načine razgovora kako bi identifikovali prijatelje, neprijatelje, policajce ili suparnike, tako se i sajber nevaljalci suočavaju sa stalnim izazovom u nastojanju da precizno ustanove „ličnu kartu" onoga s kojim ćaskaju onlajn. Deo priče u ovoj knjizi govori o tome kako su razvili metode međusobne identifikacije i

kako policija širom sveta pokušava da doskoči sposobnosti hakera da uoče agente kriminalističkih službi i takozvane tajne potkazivače (Confidential Informants, CIs) na Mreži.

Za vreme devedesetih, najjednostavniji način sprečavanja nepoželjnih gostiju da guraju nos u kriminalne aktivnosti ležao je u uvođenju strogih zabrana i sistema članstva za vebsajtove posvećene diskusijama o ilegalnim radnjama na internetu. Bez obzira na sve bezbednosne mere, posle samo nekoliko meseci ti sajtovi su prosto vrveli od pripadnika kriminalističkih službi, poput Tajne službe SAD (US Secret Service) ili obaveštajnih agencija kao što je naslednik KGB-a, FSB (Federalna služba bezbednosti Ruske Federacije), koji su dobili pristup strpljivo se pretvarajući da su kriminalci ili nakon što su ubedili potkazivače da rade za njih.

Neki agenti su glumili toliko ubedljivo da su poneke kriminalističke službe čak uložile trud da isteraju tajne policijske agente iz sestrinskih organizacija pod pretpostavkom da su zaista kriminalci.

Kao rezultat ovih napora, policija i obaveštajci su, tokom protekle decenije, sastavili obimnu bazu podataka hakera-prestupnika: ona sadrži njihove nadimke, stvarne ili pretpostavljene lokacije, tip aktivnosti u koje se upuštaju i sagovornike s kojima najčešće komuniciraju. O najnižem nivou sajber kriminalaca znaju ama baš svaku pojedinost. Ipak, uprkos svim ovim informacijama, i dalje je veoma teško podići optužnicu protiv sajber kriminalaca.

Upravo tu suštinska priroda Mreže – pogotovo njena uzajamna povezanost – stvara neverovatnu glavobolju snagama reda i zakona: niko nije sto odsto siguran s kime zapravo komunicira na Mreži. Imate li posla s običnim hakerom-prestupnikom? Ili imate posla s nekim ko ima prijatelje na visokim položajima? Razgovarate li sa kriminalcem? Ili sa potkazivačem? Ili s vojnim istraživačem koji procenjuje vrednost tehnika kriminalnog hakovanja? Da li posmatrate svog sagovornika ili on posmatra vas? Pokušava li da zaradi za sebe? Ili za Al-Kaidu?

„Ovo je poput partije sedmodimenzionalnog šaha", primetio je futurolog Bruno Gvisani, „u kojoj nikad niste sigurni ko vam je u kom trenutku protivnik."

* * *

Kad sam stigao pred sedište Googlea u Mauntin Vjuu, u Kaliforniji, nije baš bilo kao onomad kad sam prvi put ugledao Tadž Mahal, ali dok sam parkirao auto u Aveniji Čarlston, ispred višebojnog znaka koji je objavljivao jedno od čuda postindustrijskog sveta, ipak sam osetio grč strahopoštovanja.

Brzina kojom se Google stopio s našom svešću, sa svim onim usponima i padovima povezanim s kontrolisanom upotrebom narkotika, nema presedana. Jedini suparnici su mu rođaci iz porodice digitalnih džinova, poput Facebooka, Microsofta i Amazona. Međutim, čak ni ova trojka ne može da se podiči onim nivoom uspeha s kojim Google pomaže, usmerava i nadzire naš život dok njegovi porozni serveri bljuju bezbrojne milijarde bajtova traženih informacija i istovremeno gutaju i skladište individualne i kolektivne profile milijardi ljudskih bića. Ti podaci, dabome, otkrivaju o nama mnogo više nego što smo svesni. Čovek zadrhti pri samoj pomisli šta se može desiti ako informacije dospeju u pogrešne ruke. Možda već jesu...

Vedra pastelna mešavina primarnih i sekundarnih boja, poznata s logoa Googlea, ponavlja se po celom „kampusu". Često koriste meke, zaobljene ivice za definisanje velikih objekata koji su s preciznom nasumičnošću razbacani po krugu. Skulpture su osmišljene tako da na njima sedite, posmatrate ih ili se igrate njima, pa ceo kompleks podseća na ogromni dečiji vrtić ili, u zavisnosti od toga koliko ste anksiozni ili paranoični, na bizarno bajkovito selo iz serije *The Prisoner*, iz šezdesetih godina prošlog veka, u koje su slali osobe smatrane opasnošću po nacionalnu bezbednost i iz kog nije bilo moguće pobeći. Umišljam li ja to ili svi koje srećem u krugu furaju osmeh koji neodoljivo podseća na stanje transa? To istovremeno pojačava paranoično tumačenje suštine Googlea i odaje utisak da se svi malo previše trude da ne budu zli. Nisam sasvim načisto je li ovo san ili košmar.

Gotovo odahnem kad upoznam Korija Luija, Googleovog menadžera za pouzdanost i bezbednost, zato što ljudi zaduženi za obezbeđenje izgledaju ozbiljno i skloni su tajnovitosti, bez obzira na to za koga rade. Njegovo držanje je dobrodošao kontrast Googleovoj auri budističke istovetnosti i jedinstva. Elegantan Amerikanac azijskog porekla tridesetih godina, otresitog ali srdačnog ponašanja, Lui svoj sajber zanat nije učio u lagodnom

okruženju Silicijumske doline, već u mnogo grubljem, „muškijem" svetu Tajne službe Sjedinjenih Država. Google ga je regrutovao potkraj 2006, dve i po godine pre moje posete. U vreme kad je napustio tu kriminalističku službu, Kori Lui nalazio se na čelu Odeljenja za e-kriminal. Bilo je malo toga što nije znao o napadima na mreže (takozvanim provalama ili prodorima), prevarama putem kreditnih kartica, čestim DDoS napadima kadrim da onesposobe vebsajtove i mreže[2] i malveru, koji su ubrzo posle milenijuma počeli da se razmnožavaju kao pacovi u kanalizaciji. Pri tom je veoma mnogo znao o kardingu (carding), nasušnom hlebu sajber kriminala. Reč je o praksi kupovine ili prodaje ukradenih ili hakovanih podataka s kreditnih kartica, kojih se stotine hiljada razmenjuju po svetu pre no što se upotrebe za kupovinu ili podizanje gotovine sa bankomata.

Kako je Google mogao da odoli strateškom resursu kao što je Kori Lui? Nikako. A kako je Lui mogao da odoli strateškom potezu nastavka karijere u Googleu – blaga klima južnopacifičke obale Sjedinjenih Država naspram vašingtonske vlage, ledene zime i samo jedne nedelje prolećnog cvetanja; neformalna odeća Zapadne obale ili krute kragne Beltveja; novac i osećaj da si uključen u dinamičan projekat ili rad za vladu SAD? Uistinu, teško da je borba bila poštena.

Kad krenete iz San Franciska autoputem 101, Google nije jedina sajber ikona pored koje prolazite – Sun Microsistems, Yahoo! i McAfee samo su neka od brojnih čuvenih imena čija sedišta proleću pokraj prozora dok se vozite prema jugu. Što više obilazite kompanije koje se bave bezbednošću, to više nailazite na bivše državne agente iz FBI-ja, US SS-a, CIA, iz Uprave za suzbijanje droge (Drug Enforcement Administration, DEA) i Poštanskog inspektorata SAD (United States Postal Inspection Service, USPIS). Čitava četa nekadašnjih špijuna i policajaca u civilu preselila se iz kliničkog okruženja DC-ja kako bi dobro živela u Silicijumskoj dolini, privučena istim onim veličanstvenim uslovima koji su namamili filmsku industriju u Holivud.

Ovaj odliv iz državnih agencija u privatni sektor rezultuje izrazitim smetnjama za vladu. Ministarstvo finansija ulaže novac u obrazovanje sajber istražitelja koji potom, čim steknu nekoliko

2 DDoS (Distributed Denial of Service) napad jeste pokušaj napadača da učini računar nedostupnim korisnicima, tako što onesposobljava mrežu, računar ili neki drugi deo infrastrukture. (Prim. prev.)

godina iskustva, odlaze u toplije krajeve. Ipak, investicija nije sasvim uzaludna, zato što ovo dovodi do konsolidacije snažnih veza između javnog i privatnog sektora. Google nije obična privatna korporacija; u očima Bele kuće, on je strateško preimućstvo države. Poruka iz DC-ja je potpuno jasna – napadni Google, i napao si SAD. U tom kontekstu, to što neko poput Korija Luija može da podigne slušalicu i popriča sa starim drugarima u Tajnoj službi upozoravajući ih na, recimo, veliki napad na gmail, umnogome olakšava kritično važnu saradnju između javnog i privatnog sektora na internetu.

Ne znam, ali spreman sam da se kladim da se Korijev životni standard poboljšao otkako se odselio na zapad, ali opet, mora vrlo naporno da radi za njega. Google je jedna od dveju najvećih riznica podataka na svetu – druga je Fejsbuk. To ih čini unosnim poslom (oglašivači drage volje plaćaju za tajne o ličnim navikama koje otkrivaju ti podaci) i to ih čini svetim gralom za hakere koji rade za sebe, za podzemlje, za industriju i suparničke države.

Pred kraj razgovora, Kori mi je ispričao o svom prijatelju policajcu koji je uložio mnogo vremena u stvaranje prijateljstava sa hakerima. Bio je toliko uspešan da je preuzeo administraciju ogromnog nelegalnog vebsajta. „Verovatno će rado razgovarati s vama", rekao je. „Vodio je sajt pod nazivom DarkMarket." Tada sam prvi put čuo za taj sajt i za ime specijalnog agenta FBI-ja Kita Dž. Mularskog. Bio je to početak čudnog putovanja.

Nastojao sam da upoznam i intervjuišem što je moguće više središnjih likova iz prošlosti DarkMarketa, raštrkanih u desetak i više zemalja: lopova, policajaca, dvostrukih agenata, advokata, hakera, krakera i prozaičnijih prestupnika. Takođe sam pregledao hrpe sudske dokumentacije vezane za DarkMarket i osobe umešane u njega. Bivši i sadašnji sajber kriminalci i policajci snabdeli su me dodatnim dokumentima i informacijama. Nikad nisam uspeo da pristupim kompletnoj arhivi samog sajta, ali nekako mi je pošlo za rukom da se domognem njenog dobrog dela. Agent Mularski, koji je posedovao gotovo celokupnu arhivu DarkMarketa, jedina je osoba umešana u slučaj koju sam upoznao a koja je imala uvid u kompletnu dokumentaciju.

Osim te neuhvatljive arhive, neki dokumentarni dokazi – mada su bili od pomoći – nisu bili sasvim tačni; to se naročito odnosi na materijal koji su tužioci iznosili na brojnim ročištima. Po mojoj proceni, te greške nisu bile posledica nemara ili osvetoljubivosti,

niti su bile namerne. Radije, odražavale su izrazito tehničku i često zbunjujuću prirodu dokaza na suđenjima povezanim sa sajber tehnologijom. Sudije i advokati su imali muke da se prilagode ovoj specifičnoj kulturi, kao i svi koji se prvi put susreću s nezakonitim aktivnostima na Mreži.

Moji pokušaji da procenim kad sagovornik laže, ulepšava priču ili izmišlja, a kad kazuje stvarnu istinu, bili su samo delimično uspešni. Svi koje sam intervjuisao cepteli su od inteligencije, i pored toga što je ponekima manjkala čvrsta ruka na moralnom kormilu, neophodna za plovidbu mutnim vodama sajber kriminala. Međutim, što sam dublje zalazio u čudni svet DarkMarketa, shvatao sam da su različite verzije istih priča o najvažnijim delovima istorije vebsajta protivrečne i da se ne daju uskladiti. Nije bilo moguće tačno ustanoviti šta se zaista događalo među igračima i s kim su, na kraju krajeva, sarađivali.

Internet je generisao neizmerna skladišta podataka i informacija, čiji je veliki procenat bezvredan, veliki procenat još uvek nerastumačen, a jedan mali procenat opasan u svojoj lažnosti. Naša rastuća zavisnost od umreženih sistema i uzajamna povezanost usled koje pripadnici visokospecijalizovanih grupa kao što su hakeri i obaveštajni agenti migriraju između zločina, industrijske špijunaže i sajber ratovanja, znači da su dokumentovanje i pokušaj razumevanja istorije fenomena poput DarkMarketa postali intelektualni i društveni zadatak od vitalnog značaja, i pored toga što su dokazi nepotpuni, tendenciozni i raštrkani po virtualnom i stvarnom svetu.

KNJIGA PRVA

Deo I

1.
Inspektorov poziv

Jorkšir, Engleska, mart 2008.

Velečasni Endru Arun Džon nalazio se jednog jutra početkom marta 2008. u stanju blagog šoka. Nije mu ni zameriti. Ne samo da je upravo bio preživeo dugo putovanje iz Delhija ekonomskom klasom, već je to bilo dve nedelje pre otvaranja novog Terminala 5 na Hitrou, pa je najužurbaniji međunarodni aerodrom na svetu istraživao nove standarde maltretiranja putnika. Iz Indije je poleteo negde oko tri ujutru i, posle sporog vukljanja kroz pasošku kontrolu i haosa pri preuzimanju prtljaga, tek ga je čekala četvorosatna vožnja na sever do Jorkšira.

Kad je uključio mobilni telefon, velečasni Džon je video da ima neuobičajeno veliki broj propuštenih poziva od svoje žene. Pre no što je stigao da joj se javi i upita gde gori, ponovo je pozvala. Rekla mu je da je policija već nekoliko puta telefonirala i da pod hitno moraju da stupe u kontakt s njim.

Zatečen i zbunjen, velečasni je oštro odgovorio supruzi, rekavši joj da priča gluposti – mada je skoro odmah zažalio zbog svog tona.

Njegova supruga je pak, srećom, rešila da zanemari njegovu osornost. Jasno i smireno mu je objasnila kako je policija htela da ga upozori na to da mu je neko provalio tekući račun, da je stvar hitna, te da bi trebalo da što pre pozove broj nadležnog policajca koji su joj ostavili.

Suprugin poziv je još više uznemirio velečasnog i njegov iscrpljeni mozak je smesta pokrenuo sve točkiće. „Ko mi je provalio tekući račun?", pitao se. „Koji račun? Ovde kod Barklija?", nagađao je. „Moj račun u Standard banci u Južnoj Africi? Ili ICICI u Indiji? Ili možda sva tri?" Još ga je više zbunjivalo – o čemu ona zapravo govori? „*Kako* su mi to provalili račun?"

Došavši tako brzo posle iscrpljujućeg leta, čitava afera uznemirila je i iznervirala velečasnog. „Pozabaviću se time kasnije, kad stignem u Bradford i malo se odmorim", promrmljao je sebi u bradu.

Bradford se nalazi oko 320 kilometara severno od aerodroma Hitrou. Devedeset pet kilometara istočno od grada leži Skantorp, gde je mali tim policijskog detektiva Krisa Dosona nervozno iščekivao telefonski poziv velečasnog Džona. Policajca je polako obuzimao osećaj da tone u živi pesak slučaja za koji je podozrevao da je veoma krupan i koji je pred njega postavio naizgled nepremostivi problem, koji mu nikako nije ulazio u glavu. Dosad prikupljeni dokazi obuhvatali su stotine hiljada kompjuterskih fajlova, od kojih su neki bili dovoljno veliki da prime celokupna Šekspirova dela umnožena 350 puta. U tim dokumentima nalazila se planetarna biblioteka brojeva i poruka na jeziku nerazumljivom svima sem izuzetno malobrojnoj eliti širom sveta, upućenoj u tajanstvenu terminologiju sajber kriminala.

Narednik Doson možda nije znao ništa o toj novoj i vrlo retkoj oblasti kriminalističkog istraživanja, ali bio je prvoklasni detektiv odeljenja za ubistva s mnogo godina službe iza sebe. Među bezbrojnim spiskovima i nizovima brojeva jasno je uočavao mnoštvo osetljivih podataka, koji ne bi smeli da budu u posedu jedne osobe.

Ipak, kao što su ustanovili policajci u mnogim delovima sveta u prvoj deceniji XXI veka, naleteti na ovakvu riznicu informacija bilo je jedno. Pokušaj da je povežeš sa konkretnim zločinom bio je nešto sasvim drugo.

Da bi ubedio sudiju u uspavanoj varoši Skantorp na reci Hamber da produži pritvor osumnjičenom, detektiv Doson morao je da predoči kristalno jasne dokaze o konkretnom zločinu. Štaviše, uvek su postojali realni izgledi da će te dokaze predočiti nekom odrtavelom oblasnom sudiji koji ima teškoća i s daljinskim upravljačem za televizor, a kamoli s pristupanjem elektronskoj pošti. Pri tom ubedljivost nije bila dovoljna – slučaj je morao biti neprobojan i dovoljno jednostavan da ga svi razumeju.

Vreme je neumoljivo curilo. Osumnjičenog su smeli da drže u pritvoru samo tri dana, od kojih su dva već bila prošla. Među silnim fajlovima, veblogovima, četlogovima i đavo bi ga znao čime još, Doson je imao samo jednu jedinu mrvicu dokaza.

Zurio je u pedeset reči na papiru formata A4. Obuhvatale su broj bankovnog računa, 75377983; datum kad je otvoren, 24.2.2006, kao i stanje na računu, 4022,81 funte. Međutim, tu je bilo i ime: gospodin E. A. Džon; imejl adresa: STPAULS@LEGEND.CO.UK; adresa stanovanja: St Pols Roud 63, Maningam, Bradford; ime korisnika i, najvažnije od svega, lozinka za logovanje na račun: 252931.

Ako uspe da potvrdi identitet vlasnika računa, i ako taj čovek dâ izjavu kako nikad nije svesno otkrio svoju lozinku drugoj osobi, Doson će verovatno uspeti i da ubedi sudiju da pošalje optuženog na suđenje i odbije zahtev za puštanje uz kauciju. A to bi možda obezbedilo detektivu taman dovoljno vremena da shvati sa čime tačno ima posla.

Kad je pokušao da kontaktira sa gospodinom E. A. Džonom, Doson je saznao da je to sveštenik Anglikanske crkve, koji je odveo grupu siromašne dece na raspust u Indiju. Rečeno mu je i da neće moći da stupi u kontakt s njim dok se ovaj ne vrati iz Delhija. Velečasni je trebalo da stigne nekoliko sati pre no što su osumnjičenog morali da puste iz pritvora. Ako ne stigne, živi pesak ovog slučaja progutaće okean podataka na koji je naleteo Doson. A skupa s podacima, nesumnjivo će i osumnjičeni potonuti natrag u anonimnost svog virtualnog alter ega.

Na Dosonovu nesreću, velečasni je bio toliko uznemiren posle razgovora sa suprugom da je odlučio da se problemom pozabavi tek po povratku u svoju parohiju, Maningam. Štaviše, isključio je mobilni telefon i umesto toga se usredsredio na dugu vožnju od aerodroma do kuće.

Zašto se, dakle, toliko uznemirio?

Ukratko, velečasni Džon bio je čovek srdačne, vesele naravi. Rodom s oboda pustinje Tar u Radžastanu, imao je pomalo šestougaono lice čija je vedrina prosto zračila iza njegovih profesorskih naočara. Poticao je iz manjinske zajednice indijskih hrišćana i postao je sveštenik Indijske anglikanske crkve u Delhiju, u kojoj je radio petnaest godina.

Međutim, 1996. Crkva Južnoafričke oblasti ponudila mu je da preuzme upravljanje parohijom u indijskoj opštini Lenasija, četiri kilometra južno od Soveta, za vreme tranzicije s aparthejda na višepartijski sistem.

To je za svakoga bio izazovan potez, budući da su to bila teška vremena za njegov novi dom. Radost kojom je dočekan kraj

rasističkog režima bila je umanjena spoznajom koliko duboko sežu gnev i ogorčenje koji su se nagomilavali prethodne dve stotine godina. Pridošlice poput velečasnog Džona morale su posedovati sofisticirano poznavanje političke i društvene situacije da bi razumeli značaj tih tenzija i znali kako mogu pomoći da se one umanje.

Njegov uspešan rad u Južnoj Africi nije prošao neprimećeno u vrhovima hijerarhije Anglikanske crkve i, posle osam godina, biskup iz Bradforda, u engleskom okrugu Zapadni Jorkšir, predložio mu je da razmisli o podjednako izazovnom položaju u Maningamu, stambenoj četvrti na obodu gradskog centra Bradforda. Velečasni Džon je oklevao – sa svojom očajnom klimom i velikim urbanim središtima, Engleska mu je oduvek delovala kao prilično sumorno mesto.

Isto tako, znao je da Maningam nije nimalo idiličan kraj. Mnogi Britanci doživljavali su Bradford, a pogotovo Maningam, kao simbol neuspešnih pokušaja države da integriše svoje brojne etničke i verske grupacije. Oni zlonamerniji videli su u Maningamu mogućnost da podjare nepoverenje među tim zajednicama.

U julu 2001. u ovoj oblasti došlo je do kratkotrajnih ali nasilnih nereda koji su odražavali sve dublji jaz između mnogoljudne azijske populacije u gradu i njegovih belih stanovnika. Maningam je već ranije doživeo fenomen odliva belačkog stanovništva („white flight") i, kad je velečasni Džon došao tamo, sedamdeset pet procenata populacije činili su muslimani, koji su mahom vodili poreklo iz ruralnih krajeva na severoistoku Pakistana. „Preostalih dvadeset pet procenata su hrišćani, mada od toga samo oko pet procenata ide u crkvu. Belačko stanovništvo ovde izgleda i oseća se kao manjina, što i jeste", rekao je velečasni Džon. Premda klima, arhitektura i kultura nemaju nikakvih sličnosti s johanesburškim crnačkim naseljima, Maningam je po svemu ostalom sablasno podsećao na Južnu Afriku.

Nova dužnost bila je teška. Kad se nakupe oblaci ili napada sneg, malo se toga lepog moglo videti na ulicama oivičenim sumornim neogotičkim građevinama. Ipak, pre samo malo više od jednog veka, Maningam je bio veoma poželjan kraj za život. To je bilo u razdoblju koje je spoljni svet davno zaboravio, kad su Bradford, koji je bio moćan zamajac britanske industrijske revolucije, veličali kao „svetsku prestonicu vune".

Početkom dvadeset prvog veka, međutim, Maningam je već godinama propadao. Nekadašnji cvatući napredak i zaposlenost odavno su otišli odatle. Njihovo mesto zauzeli su droga, kućno nasilje, krađe, provale, paljevine i prostitucija. Velečasni Džon je u svom prihvatilištu brinuo o više ljudi – koji su svi pokušavali da izbegnu zamke siromaštva i zločina – nego što je nedeljom dolazilo u njegovu crkvu.

Uz stalnu pretnju da će latentno nasilje u nekom trenutku izbiti na površinu, rad velečasnog Džona odvijao se na prvoj liniji fronta klasnih, kulturnih i društvenih sukoba u Britaniji. Kao čovek koga nije lako uplašiti, sačuvao je spremnost da se nasmeje u najrazličitijim okolnostima. S obzirom na izazove svog svakodnevnog posla, pitao se zašto ga je vest o upadu u njegov bankovni račun toliko uznemirila. Više od svega želeo je da popriča sa svojim sinovima, koji su se razumeli u kompjutere. Potom je odlučio da što pre razgovara s policijom, kako bi saznao šta se dešava. „Pre svega", zaključio je, „hoću da se to reši i da što pre ostane iza mene."

Nervozna reakcija velečasnog nije neuobičajena. Psihološki odgovor na saznanje da smo postali žrtve sajber kriminala sličan je onome što proživljavaju žrtve provale. Mada je delo ograničeno na sajber prostor, svet mnoštva majušnih elektronskih impulsa, ipak ga doživljavamo kao fizičko nasilje. Jer, ako su vam upali u bankovni račun, šta su još lopovi možda otkrili u privatnosti vašeg kompjutera?

Da vam nisu, možda, ukrali, podatke iz pasoša, koje sada neki kriminalac ili obaveštajni agent koristi u lažnoj putnoj ispravi? Može li biti da čak i sad, dok ovo čitate, pregledaju vašu elektronsku poštu s poverljivim informacijama o kolegi ili zaposlenom? Mogu li naleteti na neke opasne ljubavne imejlove ili kakvu drugu indiskretnu prepisku koju ste slali ili primali? Postoji li ijedan deo vašeg života koji ne mogu da istraže ukoliko imaju pristup vašem kompjuteru?

Sad već krajnje odlučan, čim je stigao u udobnu malu kuću pored impozantnog tornja svoje crkve u Maningamu, velečasni Džon telefonirao je policajcu u susednom okrugu Linkolnšir.

Krajnje je neobično što je ovaj slučaj dopao baš u ruke Krisa Dosona, skantorpskog policajca u ranim srednjim godinama. Većina slučajeva sajber kriminala u Britaniji dospeva specijalnim odsecima koji rade u sastavu triju službi – Metropolitan policije

(Metropolitan Police), Policije grada Londona (City of London Police) i Agencije za krupni organizovani kriminal (Serious Organised Crime Agency, SOCA), koje se sve nalaze u prestonici. Neobučeni policajci najčešće previđaju takve slučajeve, zbog njihove ezoterične prirode. Doson je, međutim, bio neobičan: bio je pandur koji se upravljao instinktom, čijem oku ništa nije promicalo. Posedovao je i tihi šarm, ali i onu tipičnu severnoenglesku iskrenost koja je samo doprinosila njegovom metodičnom i preciznom pristupu policijskom poslu. Ta moć da zapazi detalje dobro će mu doći u narednim mesecima.

Ako se Maningam povezuje s etničkom napetošću i strmoglavim privrednim propadanjem, obližnji Skantorp (75.000 stanovnika), koji leži južno od reke Hamber, više se posmatra kao engleska nedođija i predmet sprdnje zbog svog imena[3] i večite loše igre gradskog fudbalskog tima. (Istini za ljubav, valja dodati da grad barem nije nasledio svoje prvobitno skandinavsko ime, Skumtorp,[4] a da je fudbalski klub Skantorp junajted, sve dok maja 2011. nije prešao u niži rang takmičenja, bio neravnopravne bitke u engleskoj drugoj ligi.) Koliko je moguće ustanoviti, ova varoš se nikad nije pominjala u vezi s nekom opsežnom kriminalnom aktivnošću.

Samo četiri dana pre povratka velečasnog Džona s njegovog dobrotvornog rada u Indiji, detektiv Doson je zadovoljno obavljao svoj posao u skantorpskoj glavnoj policijskoj stanici. Posmatrao je Dnevnik zapovesti i nadzora (Command and Control Log), kompjuterski ekran koji prenosi podatke o telefonskim prijavama. Standardni sadržaj obuhvatao je prekršaje u pijanom stanju, povremeno kućno nasilje i mače koje ne ume da siđe s drveta. Međutim, te srede u pola dva po podne, u dnevniku se pojavila poruka koja je zagolicala narednikovu radoznalost. Izrazito je odskakala od uobičajenog. Okrenuo se i, svojim pevuckavim linkolnširskim naglaskom, blago se obratio kolegi: „Ajde, onda. Bolje da odemo i pogledamo o čemu je reč. Izgleda da se u Grimley Smithu događa nešto sumnjivo."

3 Eng. *cunt* je vulgarni naziv za ženski polni organ, zbog čega je AOL-ov filter za opscenosti još 1996. odbijao da prihvata ukucavanje imena ovoga grada. Neki forumi prikazuju ga kao *S****horpe*, dok se ponegde piše kao *Scoonthorpe*. Ta vrsta besmislene cenzure postala je u kompjuterskom svetu poznata kao *Scunthorpe Problem*. (Prim. prev.)

4 Eng. *scum* je žargonski izraz za šljam, ološ, propalitet i tome slično. (Prim. prev.)

2.
Miranda priča o hrabrom novom svetu

Na vebsajtu Grimley Smith Associatesa prikazana je fotografija u sepiji na kojoj se vidi njihovo sedište, onako kako je izgledalo u edvardijanskim vremenima, kad se u njemu nalazio prvi salon automobila u Skantorpu. Čudno je, ali firma ponosno reklamira belsajz, davnašnji simbol automobilskog šika u Britaniji, čiji je proizvođač bankrotirao ubrzo posle Prvog svetskog rata. Međutim, ta časna starina i dikensovsko ime Grimley Smith predstavljaju varku. GSA je, naime, kao što svi dobro znaju, osnovana relativno nedavne 1992. godine, kao ortačka firma gospodina Grimlija i gospodina Smita.

Kompanija pruža daleko složenije tehničke usluge od prodaje i popravke starih krntija. Specijalizovana je za aplikacije iz oblasti hemijskog inženjerstva za energetsku i farmaceutsku industriju, i na glasu kao jedna od najuspešnijih mladih skantorpskih kompanija, koja sad može da se podiči i svetskim prisustvom.

Dvojica osnivača GSA bila su u početku i jedina radna snaga, koja je u međuvremenu narasla na više desetina školovanih inženjera i tehničara. Poput svih biznisa u kojima uspeh podstiče ekspanziju, razvoj GSA odvijao se uzbudljivo ali nasumično. Njihovi inženjeri angažovani su za rad na mamutskim projektima u međusobno veoma udaljenim mestima kao što su Iran, Kina i Venecuela. Specijalistička priroda njihovog posla i nedopustivost ikakvih grešaka u njihovim proračunima zahtevala je neke moćne kompjuterske programe. Konkretno, koristili su takozvani CAD (Computer-Aided Design, kompjuterski potpomognut dizajn) softver, koji je omogućavao složene 2D i 3D simulacije projekata.

Sredinom 2007. kompanija je dosegla fazu kad joj je bilo očajnički potrebno upravljanje kompjuterskom infrastrukturom. Angažovanje firme koja se bavi održavanjem i bezbednošću kompjuterskih sistema ispostavilo se kao skupa opcija, pa je rukovođenje raznoraznim sajber potrebama kompanije postajalo

sve teže. Direktori su se zato opredelili za novi pristup celom sistemu.

Pravog čoveka za taj posao našli su u Derilu Liningu, opuštenom lokalnom momku. Osim što je posedovao tehničku stručnost, bio je mlad, neumoljivo pošten, ali možda je najvažnije bilo to što je njegovo ležerno, prijateljsko ponašanje prikrivalo nesvakidašnje prodoran um. Naime, činjenica o kojoj se ne vodi mnogo računa jeste da najbolji kompjuterski menadžeri izlaze na kraj sa društvenim i psihološkim očekivanjima isto tako uspešno kao s popravkom softverskih aplikacija.

Čim je prvi put kročio u kancelariju, Deril je shvatio da se smesta mora pozabaviti kompjuterima Grimley Smitha. Najviše ga je brinulo to što je svaki član osoblja imao „administratorska prava" na računaru na svom radnom mestu. Smeli su da instaliraju svaki program koji požele i da koriste sve onlajn usluge koje hoće (sem pornografskog materijala, koji je prethodni IT režim centralno blokirao).

Na porodičnom kompjuteru, administrator je obično samo jedna osoba (roditelj). On će odabrati, na primer, da elektronski ograniči količinu vremena koje drugi članovi porodice provode za kompjuterom ili tip vebsajtova koje smeju da posećuju.

Jedna od najvažnijih „povlastica" koje porodični PC daje administratoru tiče se instalacije novih softverskih programa. Na taj način, roditelji mogu da spreče decu da igraju igrice koje smatraju nepodesnim. Međutim, tu povlasticu mogu da iskoriste i za sprečavanje „skidanja" softvera sumnjivog porekla, zato što program može sadržavati virus ili drugi zlonamerni materijal koji bi učinio ceo digitalni svet porodice podložnim napadu.

Ista načela važe i u poslovnom okruženju, samo obično u većim i složenijim razmerama. Prvi problem s kojim se Deril suočio kad je počeo da radi u Grimley Smithu bilo je odsustvo centralnog administratora. Ne može se tolerisati u savremenom poslovanju, uporno je govorio direktorima, da osoblje kači na internet, skida ili instalira šta god poželi.

Rekao im je da je centralna kontrola od suštinskog značaja za sprečavanje ljudi da ne znajući omoguće virusima da probiju odbranu mreže. Objasnio je da se zaposlenima, po svoj prilici, može u potpunosti verovati – ne ugrađuješ antivirus softver u svoj sistem zato što sumnjaš kako tvoje kolege žele da ga zaraze, jer uglavnom ne žele. Isto važi, nastavio je, za pitanje instalacije

softvera i svega ostalog, što se toga tiče. Vrednost podataka u visokospecijalizovanoj kompaniji kao što je GSA zapravo je nemoguće izračunati. Ako padnu u pogrešne ruke, to može da uništi kompaniju.

Deril se u svom krstaškom pohodu čišćenja kompjuterskog sistema Grimley Smitha od škodljivih ranjivih tačaka – onih nevidljivih digitalnih rupa kroz koje bi se neprimećeni mogli provući crvi, trojanci i virusi – suočio s određenim problemima. Prvo, bilo mu je jasno da se ljudi odupiru oduzimanju povlastica koje već uživaju – a ako se izuzmu naga tela što se uvijaju na ekranu, osoblje GSA uživalo je u mnogo čemu. Za jednog mladog stručnjaka, Deril je pokazivao odlično razumevanje psihologije povezane s korišćenjem kompjutera. Morao je da nađe načina da odvikne osoblje od njihovih prava lokalnog administratora. Rešio je da će biti najbolje da to radi postepeno. Znao je da ljudi ne vole da gube ono što već imaju, ali je potom razborito zaključio kako im je isto tako drago da dobijaju nove igračke.

Stoga je iskoristio prvo sledeće unapređenje kompjutera kao priliku da uvede prva ograničenja. Oduševljeni svojim šljaštećim i izuzetno moćnim novim mašinama, zaposleni u GSA spremno su prihvatili činjenicu da više ne mogu da skidaju omiljene igrice ili razonode kad god im se prohte.

Ponovo ispoljivši urođeni dar za psihologiju, Deril je izbegavao preterano drakonske metode. Problem je predstavljao Fejsbuk. Mnogo zaposlenih je uludo trošilo vreme boraveći na društvenim mrežama onda kad bi trebalo da rade. Međutim, to je sve više prerastalo u ono što bezbednosna industrija naziva „vektorom" napada – instrument koji tvorci virusa mogu zaposesti kako bi krčmili svoju robu.

Deril je smatrao da bi potpuna zabrana Fejsbuka mogla dovesti do pobune u firmi, pa je umesto toga dozvolio pristup tom sajtu od podneva do dva po podne, kad je većina zaposlenih koristila pauzu za ručak. Time što je lično odredio vreme za korišćenje Fejsbuka, bilo mu je lakše da prati pokušaje ubacivanja malvera i hakovanja, i osigura da sajt ne ugrozi bezbednost kompanije.

Bez velike buke uveo je sistem relativno jake centralne kontrole, ne otuđivši pri tom nijednog korisnika kompjutera u Grimley Smithu. U srcu novog poretka nalazio se složeni program pod nazivom Virtual Network Computing ili VNC. Bila je to Grimley Smithova sopstvena verzija Velikog brata. Ukoliko Deril

identifikuje bilo kakvo neobično ili preteće ponašanje u sklopu sistema, mogao je da pokrene VNC iz virtualne hibernacije i pusti ga da detaljno ispita šta se dešava na svakom od desetina kompjutera kojima je sada upravljao.

Jednog jutra, nakon što se osoblje ulogovalo na svoje kompjutere, Deril je poslao poruku kojom je upozoravao sve, od generalnog direktora naniže, da će odsada svi biti podvrgnuti skriningu od strane menadžera kompjuterskog sistema. Ono što većina nije znala bilo je da u pozadini veselo pevuši Derilov novoinstalirani VNC. Ukoliko se pojavi upozorenje da je neko učitao s interneta virus ili da pokušava da instalira neki nepoznati softver, VNC će se aktivirati.

VNC je vrlo moćna alatka. Nekima njegova upotreba deluje kao normalna poslovna praksa, ali na globalnom internetu, angažovanje VNC softvera se žestoko osporava. U velikom delu kontinentalne Evrope, državnim institucijama i kompanijama je strogo zabranjeno da pristupaju svim informacijama na kompjuterima zaposlenih koje nisu povezane s poslom (a čak ni to nije lako). Nadziranje elektronske pošte je potpuno nezakonito.

Razotkrivanje zločina i građanske slobode nikad se nisu baš lagodno družili, ali njihova koegzistencija postala je znatno nezgodnija od širenja interneta, a tako će se nastaviti i ubuduće. U Nemačkoj, ako policajac anonimno prati osumnjičenog preko interneta, zakon ga obavezuje da se identifikuje kao pripadnik kriminalističke službe ukoliko onlajn sagovornik to zatraži. To veoma otežava uvreženu praksu u Britaniji i Sjedinjenim Državama, gde se policajci predstavljaju kao maloletni dečaci i devojčice kako bi uhvatili pedofile koji se sa zadnjim namerama sprijateljuju s decom u onlajn kontaktu. Upotreba VNC-ja ima politički naboj i važni zakoni o zaštiti podataka je ograničavaju. Stoga je Deril Lining morao veoma obazrivo da barata svojim ljubimčetom.

Jednog dana početkom februara 2008, na Derilovom ekranu zasvetleo je signal koji je upozoravao na sumnjivi softver. *Unauthorised Application: Messenger* (Neodobrena aplikacija: mesindžer). Derilovi sistemi motrili su na pojavu nekoliko različitih tipova neodobrenih aplikacija. Reč „messenger" nagoveštavala je da neko pokušava da instalira ili upotrebi neki oblik komunikacijskog paketa poput Skajpa. U roku od nekoliko minuta, Deril je ispratio njen trag do hemijskog inženjera koji je predstavljao istinski oslonac firme. Idući do njegovog radnog mesta, Deril je

odlučio da ga prosto pita je li na svom kompjuteru pokrenuo novi instant mesindžer.

„Okrenuo se prema meni i prezrivo odvratio: 'Nisam!' Glatko je porekao. Stoga sam odvratio: 'O, pa dobro. Mada je čudno, jer sam maločas dobio upozorenje da je ovaj kompjuter pokrenuo neodobrenu mesindžer aplikaciju.'"

Deril je slegao ramenima. Inženjerov odgovor nije ga previše iznenadio, zato što su kompjuterski sistemi osetljivi uređaji, a on je, po sopstvenom priznanju, imao instalirane raznorazne alatke za skeniranje, koje su njegovom antimalver softveru ličile na instrumente za hakovanje. U svakom slučaju, smatrao je Deril, čak i ako je inženjer pokrenuo taj program, verovatno samo četuje s društvom u radno vreme. Sada će barem shvatiti da to nije u redu, da ga Deril posmatra i da će znati ako ga ponovo upotrebi. Stoga je prosto zaboravio na to.

Dve nedelje kasnije, međutim, ponovilo se. Ovog puta, rešio je Deril, probudiće moćnu VNC zver. Ušavši u inženjerov kompjuter, počeo je da ga pretražuje u potrazi za programom za komunikaciju – koji je brzo identifikovao kao Miranda Instant Messaging. Danas mnogi koriste instant mesindžere, koji im omogućavaju da razgovaraju s prijateljima u realnom vremenu tako što unose nekoliko reči ili rečenica u mala polja za unos. U većini slučajeva, Windows Instant Messenger (IM) može da komunicira samo s onim ko ima isti softver. Prednost Mirande leži u tome što možete da komunicirate s mnoštvom različitih IM programa. Naročito je omiljena među opsesivnim korisnicima kompjutera.

Pre no što je pokrenuo VNC, Deril je proverio inženjerov hard disk, da vidi može li uočiti išta neobično, ali se potraga ispostavila kao jalova. Bilo je oko 12 i 15, vreme ručka. Baš pravo vreme, pomislio je Deril, za malu VNC sesiju na njegovoj mašini, kako bi jednom zasvagda utvrdio da li je taj neodobreni program zaista aktivan u inženjerovom kompjuteru.

Miranda IM nije bila ništa u poređenju s onim što je Deril video kad je VNC počeo da istražuje tajne inženjerovog kompjutera. Inženjer je bio otvorio deset tekst dokumenata istovremeno i skrolovao ih je nenormalnom brzinom. Deril je zinuo od čuda. Još nikad nije naišao ni na koga kadrog da takvom brzinom radi s dokumentima. Posmatrajući inženjerov ekran, video je samo mutne mrlje od brojeva, simbola i reči. Polako je shvatao da inženjer kopira delove dokumenta i potom ih nalepljuje u zasebni wordpad fajl.

Još mu nije bilo jasno šta se događa niti odakle dolaze svi ti dokumenti, ali koliko je mogao da vidi, ništa od toga nije ni izdaleka ličilo na bilo šta vezano za poslovanje kompanije. Naziv fajla u koji je inženjer nalepljivao tekst bio je zbunjujući. Zvao se „Sijera Leone". Inženjer je zaista radio na projektu rafinerije u Sijera Leoneu. Deril je ispustio duboki uzdah olakšanja – možda je čitava rabota ipak sasvim legitimna. Tek kasnije mu je sinulo zašto je inženjer odabrao baš to ime. Ako neko prođe pored njegovog kompjutera, samo bi uvukao fajl, a na liniji zadataka video se samo jezičak s nazivom „Sijera Leone": baš projekt na kom je radio.

I Derila bi to zavaralo da VNC tada nije uočio neregistrovanu memorijsku jedinicu – F: - što je ukazivalo da inženjer koristi nekakav prenosivi disk. Deril je poslao VNC u tajanstvenu memorijsku jedinicu i naložio mu da kopira desetine hiljada fajlova koje je tamo pronašao.

Kako nije bio siguran šta mu je dalje činiti, a još se nije nalazio u položaju da ustanovi šta se kog đavola događa, Deril je svom vernom VNC-ju naložio da još jednom istraži unutrašnjost sumnjivog kompjutera. Programirao ga je da svakih trideset sekundi pravi skrin-šotove inženjerovog PC-ja. Gledanje u kompjuter u realnom vremenu potpuno ga je zbunilo. Bilo je nemoguće identifikovati šta ti podaci zapravo predstavljaju. Međutim, kad je video skrin-šotove – statične slike inženjerove aktivnosti – stekao je prilično dobru predstavu šta je posredi: bile su to stotine i stotine brojeva kreditnih kartica, bankovnih računa, ličnih podataka, PIN-ova i imejl adresa. Ništa od toga nije imalo ama baš nikakve veze s razvojem naftno-prerađivačkih kapaciteta Sijera Leonea.

Potom je Deril odštampao jednu naročito punu stranicu podataka iz Bank of Amerika onlajn (Bank of America Online) i odneo je svom direktoru Majku Smitu. Ovaj je posle samo nekoliko minuta uzeo telefon i pozvao policiju u Skantorpu.

Kad je detektiv Doson stigao u Grimley Smith, direktor mu je pokazao odštampane papire. Bilo je tu svakakvih podataka, da ti se zavrti u glavi: informacije o bankama, agentima za kupoprodaju nekretnina, osiguravajućim društvima, tematskim parkovima, bioskopima, dobrotvornim organizacijama i čemu sve ne, uključujući i nešto što je ličilo na podatke dobijene od vojnih službi SAD. Smesta je posumnjao da ima posla s nekom vrstom prevare, ali nije

mogao znati šta sve to znači niti odakle da počne kako bi potvrdio svoje sumnje. Bila su to teška pitanja.

„Dobro", rekao je Doson. „Hajde da ga pozovemo u kancelariju i popričamo s njim, važi?"

Direktori Grimley Smitha su se nervozno zgledali.

„Šta je bilo?", upitao je Doson.

„On je prilično krupan momak", stigao je odgovor, „i siguran sam da dobro udara."

„Pa, taj most ćemo preći kada do njega dođemo", rekao je Doson, onoliko autoritativno koliko je mogao.

Međutim, visok, impozantni muškarac ušao je u kancelariju izgledajući više preneraženo nego ljutito. S nagoveštajem prezrenja se obratio detektivu i upitao ga ko je i šta traži tu. Doson je objasnio zašto su ga pozvali u GSA i bez uvijanja upitao čoveka šta znači sva ta dokumentacija. Ovaj je pak neočekivano ravnodušno odvratio kako je to deo izveštaja koji sastavlja za jednog od prisutnih direktora. Usledio je trenutak tišine pre no što je direktor prkosno odvratio: „Ne, nije!"

„U redu", rekao je Doson, „ispružite ruke, gospodine." Potom je klimnuo glavom kolegi: „Stavi mu lisice!"

Daleko od „dobrog udaranja" kog su se pribojavali direktori, čovek je sve vreme bio potpuno miran, iako malčice zabezeknut. Dva sata nakon što je dobio izveštaj o Zapovestima i nadzoru, Doson je imao osumnjičenog u zatvorskoj ćeliji. Međutim, morao je vrlo brzo da izgradi slučaj. Ako u roku od tri dana ne uspe da sakupi preliminarne dokaze o zaveri ili prevari, moraće da pusti čoveka na slobodu, a to će biti kraj cele priče.

Detektiv se vratio u Grimley Smith sa službenikom iz odeljenja za održavanje sistema i, zajedno s Derilom Liningom, dali su se na posao. Kao što je Deril i predvideo, na prenosive diskove bile su spakovane stotine hiljada dokumenata, a većina je bila krcata pojedinostima o hakovanim kreditnim karticama i bankovnim računima. Međutim, bilo je tu i elektronske prepiske koja se, između ostalog, odnosila i na diskusionu grupu na Yahoo!-u, prozaično nazvanu *bankfraud@yahoogroups.com*.[5] Postovi i razne

5 Eng. *bank fraud* – „bankarska prevara", izraz koji označava upotrebu potencijalno nezakonitih sredstava za dolaženje do novca, vrednosti ili druge imovine u posedu ili držanju banke, ili uzimanje novca od deponenata (vlasnika štednih i tekućih računa i sl.) tako što se prevarant lažno predstavlja kao banka. (Prim. prev.)

poruke ove grupe nisu bili puko onlajn uputstvo već prave studije na temu kako izvesti internet prevaru.

Doson se potom odvezao u stan u ulici Plimsol, u obližnjem Halu, gde je osumnjičeni živeo. Adresa se nalazila u stambenom bloku, očigledno sagrađenom u sklopu plana za obnovu kvartova na dokovima, a zgrada je već pokazivala prve znake propadanja. Fasadu krem boje naruživali su prljavi tragovi vode i bila je puna mrlja od rđe što je izbijala od armature. Bio je to odgovarajući fizički simbol Britanije novog laburizma – spolja sve sjajno i bajno, ali nesposobno da spreči trulu unutrašnjost da izbija kroz površinu.

Sve u stanu je odavalo da tu živi neženja. Ni slučajno nije bio svinjac, ali stvari su bile razbacane naokolo. „Nema tu ženske ruke", pomislio je Doson. A onda, u spavaćoj sobi, detektiv je našao ono što je tražio. Na krevetu su se nalazila dva laptopa, od kojih je jedan još bio uključen. Na njemu se nalazila hrpa dokumentacije, koja je obuhvatala bezbrojne priznanice Vestern unionа koje su potvrđivale transfere po celom svetu: Novi Zeland, Meksiko, Ujedinjeni Arapski Emirati, Ukrajina – svuda i odasvud.

Međutim, i pored svih tih fajlova i dokumenata, Dosonu su, kao što znamo, bili potrebni dokazi o konkretnom zločinu da bi podigao optužnicu. Kad je podigao debeli svežanj papira, iz njega je ispao jedan list i odlepršao na pod. U narednim mesecima, Doson je često razmišljao o srećnoj slučajnosti koja je baš u tom trenutku rešila da ga snađe. Naime, na tom listu papira nalazili su se podaci gospodina koji živi negde u Zapadnom Jorkširu, skupa sa svim brojevima vezanim za njegov bankovni račun. Nakon što ga je proučio, Doson je shvatio da bi to mogao da bude onaj vitalno važni ubedljivi dokaz, zato što se tu nalazila i lozinka. Ako uspe da dokaže da taj čovek nikad nikom nije otkrio svoju lozinku, tada će možda i imati slučaj. Zato je detektiv Doson jedva čekao da porazgovara s velečasnim Endruom Arunom Džonom. Ako Džon to potvrdi, Doson će moći da optuži osumnjičenog za konkretan zločin prevare putem interneta, a sudija će skoro sigurno odbiti puštanje uz kauciju. Doson će potom moći da se lati herkulovskog zadatka da pregazi ovaj okean dokumentacije.

3.
Gospodin Hajd iz Lagosa

Adevale Taivo je 2003. diplomirao hemijski inženjering na Univerzitetu u Lagosu. Sin univerzitetskog profesora i državne činovnice, Adevale je bio visok i zgodan, i izrastao je u artikulisanog i odmerenog mladog čoveka s obećavajućom budućnošću u industriji ili akademskom svetu. Porodica je, po nigerijskim standardima, bila dobrostojeća, a imali su i rodbinu u Londonu, kadru da pomogne Adevalu kad je istraživao mogućnost da nastavi školovanje u Ujedinjenom Kraljevstvu.

Bila je to i godina kad je stvorio svoj alter ego – Fred Braun iz Oldama, u Lankaširu. Premda Adevale još nikad nije bio u Engleskoj, odlučio je da unapred stvori tog istinskog gospodina Hajda sajber sveta. Upravo je Fred Braun bio osnivač diskusione grupe na Yahoo!-u koja se bavila bankarskim prevarama.

Nije prošlo mnogo, a Fred Braun je objavio i oglase na internetu koristeći sajtove kao što su *Hacker Magazine*, *Alt 2600* ili *UK Finance*:

> DOBRA PRILIKA: Poslovna prilika za ljude zaposlene u štedno-kreditnim bankama ili čiji rođaci i prijatelji rade u tim bankama da uđu u ortački posao. Poželjne banke su HSBC, Kraljevska banka Škotske, ali i druge dolaze u obzir. Molim odgovoriti Fredu B. Braunu preko Yahoo!-a, ICQ-a ili Safemaila.

Programi za trenutno slanje poruka ICQ (izvedeno iz „I Seek You") i nešto stariji IRC (Internet Relay Chat) omiljene su alatke hakera i krakera, kako se ponekad nazivaju hakeri prestupnici. To su servisi za slanje trenutnih poruka putem kojih možete ćaskati s jednom ili više osoba. Hakerima je važno to što su „dinamični", što znači da ne ostavljaju trag o razgovorima koji se preko njih vode, osim ako ih neko namerno ne čuva. Safemail je šifrovani imejl sistem koji je nemoguće krekovati. To jest, osim ako ne ubedite izraelski sud da izda nalog za predaju informacija koje

tražite, budući da se nalazi u posedu i pod upravom kompanije u Tel Avivu.

Oni koji su se javili na oglas Freda Brauna pozvani su potom da se pridruže *bankfraud@yahoogroups.com*, čiji su ciljevi i etos bili eksplicitni: „Ova grupa je za ljude koji ne žele da posluju po zakonu nego za pare i spremni su da krše pravila. Ova grupa će vas naučiti kako da varate banke i kradete identitet." Fred je mogao da tako otvoreno reklamira svoj biznis upravo zahvaljujući raširenosti nepoštenih aktivnosti na Mreži. Proći će nekoliko godina pre no što ga uoči policija, a i to samo zbog toga što je naposletku napravio nekarakteristično glupu grešku.

Fredovi oglasi bili su osmišljeni tako da operuša narod na onaj najtradicionalniji način – tako što će angažovati pomoć „iznutra". Ako ubediš službenika banke da ukrade i potom ti preda podatke o klijentima, poštedeo si sebe gnjavaže krekovanja računa ili kreditnih kartica. Počinioci prevara putem interneta ulažu veliki trud u nastojanje da pronađu nezadovoljne ili siromašne službenike banke, zato što ti rad s insajderom može dramatično povećati zaradu. Naoružan podacima s računa, kriminalac mu može pristupiti preko interneta isto tako lako kao svom vlastitom, i potom prebaciti gotovinu na račun koji je za to odredio. Sem ako uljezu nije brzo potrebna velika suma novca, omiljeni metod krađe podrazumeva podizanje malih količina tokom dužeg vremena, tako da ne primete ni banka ni klijent.

Fred Braun je, međutim, razvijao i neke naprednije metode prevara. Uspeo je da zađe još dublje u sistem banke, gde je mogao da se upušta u radnje kao što je povećavanje dozvoljenog prekoračenja. Očigledno je znao kako da promeni imena i adrese i, dabome, kako da pronađe lozinke.

Time što je udario temelje svog poslovanja još pre no što je došao u Ujedinjeno Kraljevstvo, Fred je demonstrirao svoj sistematični pristup biznisu. Bio je promišljen; nije bio društveno nesiguran; i nije trošio mnogo vremena igrajući kompjuterske igrice. Fred Braun (Fred Brown, poznat i kao Freddy Brown, Fred B. Brown, Freddy B, FredB i Freddybb) smatrao je internet jednostavnim i lakim načinom da od bezbroj ljudi na prevaru uzme velike sume novca.

Međutim, pre no što se Fred obrušio na Mrežu, njegov doktor Džekil – Adevale Taivo – morao je da se pobrine za neke druge stvari, to jest, da provede godinu dana na master studijama

hemijskog inženjeringa na Univerzitetu u Mančesteru, gde je stigao u oktobru 2005. Mesec dana pre no što je maja 2006. dobio diplomu, otvorio je račun u Londonskoj berzi zlata (London Gold Exchange, LGE), u koju je mogao da prebacuje novac iz bilo koje štedno-kreditne banke.[6]

Deponovanim novcem LGE kupuje zlato i daje vam kredite u „digitalnoj valuti". Sa sedištem u Belizeu i zlatom pohranjenim u Švajcarskoj, pogrešno nazvana Berza zlata bila je jedna od nekoliko institucija koje su se razvile devedesetih godina prošlog veka i postale omiljene među prevarantima i peračima novca. Nakon što bi prebacio svoj novac u Londonsku berzu zlata, Taivo ga je slao na račun koji je imao u sličnoj instituciji, E-Gold, odakle je preko Vestern uniona distribuirao gotovinu po svetu, bilo u svrhu pranja ili plaćanja svojim saučesnicima.

Kao i u svemu drugom što je radio, i tu se pokazao kao pedantan i efikasan: odličan student i odličan kriminalac. Grimley Smith ga je regrutovao kao prvoklasni kadar čim mu je Mančester dao master diplomu – u isto vreme kad ga je i bratstvo internet prevaranata pozdravilo kao ozbiljnog igrača.

Adevale Taivo je bio talentovani hemijski inženjer. Iako je još bio u svojim dvadesetim godinama, u Grimley Smithu su ga smatrali velikim potencijalom i nije prošlo mnogo a već su ga slali da obavlja poslove čak u Kini i Venecueli. Oblačio se dobro, ali nikad razmetljivo, a njegov BMW odgovarao je njegovoj plati i načinu življenja. Oba svoja života je vrlo ozbiljno shvatao i, dabome, njegov zakoniti posao bio je sasvim verodostojna maska koja je štitila njegove podzemne aktivnosti. Ugledna i uspešna kompanija iz energetskog sektora jedno je od poslednjih mesta gde bi čovek tražio krupnog sajber kriminalca, a pogotovo ne među njenim najvrednijim i najškolovanijim inženjerima.

Kad je detektiv Kris Doson počeo da zagleda razmere prevare Freda Brauna, zabezeknuo se. Čak i nakon što je suzio dokazni materijal, još je pred sobom imao nekih 34.000 fajlova, od kojih su poneki brojali 100-150 stranica. Na samom početku, uočio je fajl od 100 strana, krcat brojevima američkih kreditnih kartica, zajedno sa bezbednosnim kodovima i svim potrebnim lozinkama.

Detektiv Doson bavio se ubistvima – nikada dotad niko u Hambersajdu nije radio na najsavremenijoj internet prevari, a on

6 Od 26. septembra 2011. na sajtu ove ustanove stoji obaveštenje da je trajno zatvorena, zbog „teškoća u poslovanju". (Prim. prev.)

i njegov kolega na slučaju morali su da obavljaju i svoj redovni posao. Naprosto nije znao odakle da počne. Zajedno sa fajlovima, bio je tu i softver za MSR206. Taj uređaj je verovatno najvažnije oružje u arsenalu prevaranata koji rade s kreditnim karticama, poznatih pod generičkim imenom „karderi". Pomoću njega, karder može da „klonira" kreditnu karticu. To podrazumeva kopiranje svih podataka s magnetne trake pozadi i njihov prenos na komad prazne bele plastike s praznom magnetnom trakom. MSR206 je lična kovnica novca.

Doson je na fajlovima pronašao i trojance za kilogovanje.[7] Za hakera-prestupnika oni su isto što i kalauz za provalnika. Prvi virusi bili su nešto mnogo drugačije od kilogera. Kad su virusi, devedesetih godina prošlog veka, prvi put počeli da cirkulišu u velikom broju, osmišljavali su ih studenti i pubertetlije, takozvani skript klinci (script kiddies), koji su želeli da dokažu svoje umeće kao anarhični programeri. Razdražujuće je bilo to što su odlučili da to urade tako što će pričinjavati probleme što je moguće većem broju korisnika kompjutera na svetu.

Kad se vaš kompjuter zarazi, može se ponašati na najrazličitije načine: može da uspori; ako zatražite neku aplikaciju, recimo, *Majkrosoft vord*, umesto njega će se otvoriti internet pretraživač; kompjuter će se automatski gasiti; i, što je najgore od svega, može vam uništiti sve fajlove i podatke. Poznate su priče o piscima koji su zbog nekog nestašnog virusa izgubili čitave rukopise, i o statističarima koji su svojim očima posmatrali kako im nevaljali digitalni crv proždire više meseci prikupljane podatke.[8]

Međutim, posle smene milenijuma, hakeri, krakeri i kriminalci počeli su da shvataju da se virusi, trojanci i crvi mogu upotrebiti i na unosniji način. Rođen je kiloger (key logger), koji se velikom brzinom raširio po internetu. Kad se ovaj mališa jednom ugnezdi u vašem kompjuteru, njegov posao je da prati svaki vaš

7 Eng. *keylogging*; praćenje tastera (*keys*) koje za određene radnje (kucanje lozinki i sl.) pritiska korisnik kompjutera. (Prim. prev.)

8 Najjednostavnija, mada ne i sva razlika između virusa, crva i trojanaca, poznatih pod zajedničkim nazivom zlonamerni softver (malicious software tj. malware), leži u metodu njihovog prenosa – virusi se prenose putem zaraženih imejl priloga, trojanci putem sadržaja „skinutog" s interneta, dok crvi poseduju sposobnost da se samoreprodukuju na kompjuteru domaćinu i potom koriste komunikacijske programe tog kompjutera za širenje na druge mašine. Suština je, međutim, u tome da svi imaju zadatak da naškode vašem kompjuteru. (Prim. aut.)

pritisak na tastaturu. Stoga, kad otkucate *www.hsbc.co.uk*, on tu informaciju šalje svom Tvorcu ili Vlasniku, koji se može nalaziti bilo gde u svetu. Ako potom još ukucate i svoju lozinku, recimo, Robinhud, program za upravljanje datotekama virusa u Nju Džersiju, Rostoku, Lilongveu ili najcrnjim zabitima Ruritanije[9] odmah će je zabeležiti. Bingo! *Osećaj se kao u svojoj kući!* Ili, tačnije: *Osećaj se kao na svom bankovnom računu!*

Baš kao što posedovanje hiljada podataka s kreditnih kartica i brojeva bankovnih računa u ličnom kompjuteru nije zločin, nije kažnjivo ni ako imate uskladišten kiloger virus. To može da bude snažan pokazatelj kriminalne aktivnosti, ali nedovoljno da se izgradi slučaj. Kopajući po beskrajnim fajlovima, Doson i njegov kolega morali su da raspetljavaju stotine zamršenih niti.

Nakon što su u Ekselovu tabelu ručno uneli nekoliko hiljada podataka o bankovnim računima, policajci su odlučili da se jave bankama. Krajnje razumno, pomislio bi čovek, jer, najzad, ipak su bezbednosni sistemi banaka oni koje je Fred Braun tako uspešno provalio.

Razmislite još jednom.

Doson je u svojim raspitivanjima neretko naletao na zid ćutanja, zato što se banke jednostavno nisu potrudile da mu odgovore. Detektivu je manjkalo vremena za istragu, a mnogo ga je gubio na uzaludne pokušaje da ubedi banke da sarađuju.

Stav većine banaka o sajber kriminalu je nejasan. Upravo dok pišem ovu knjigu, telefonirao mi je džentlmen iz moje banke, NatVest, i upitao me jesam li u poslednje vreme kupovao neki nakit u Sofiji, glavnom gradu Bugarske. Štaviše, pitao je i jesam li platio švajcarskom Telekomu račun u iznosu od 4.000 franaka. *Rekao sam da nisam. Na to mi je saopštio da je moja NatVestova Visa kartica ugrožena, te da će mi biti potrebna nova, ali da ništa ne brinem, jer će NatVest stornirati onih 3.000 funti koje su na prevaru podignute s mog računa. Kao i svima drugima koji dožive tako nešto, silno mi je laknulo kad me je banka ljubazno uverila da neće biti nikakvih posledica po moj džep.*

Ali ko zapravo plaća za to? Banka? Ne, one su osigurane protiv takvih gubitaka. Osiguravajuće društvo? Ne, zato što oni određuju takav nivo premija koji obezbeđuje da nikad ne gube. Možda je to ipak banka, s obzirom da na to plaća premije? Da. Međutim,

9 Izmišljena srednjoevropska zemlja iz romana Entonija Houpa. (Prim. prev.)

banke vraćaju taj novac tako što naplaćuju dodatne troškove svim klijentima. U suštini, za bankovnu prevaru plaćaju svi klijenti banke.

Sasvim je razumljivo da banke ne žele da udaraju tako nešto na sva zvona. Isto tako, ne vole da javnost sazna kolika je zapravo učestalost upada sajber kriminalaca u njihove sisteme. Novinarima je nemoguće da od banaka dobiju ikakve informacije o sajber napadima kojima su svakodnevno izložene. To se još i dâ razumeti. Ono za šta pak nema baš tolikog opravdanja jeste oklevanje da sarađuju s policijom, u slučaju da se informacija obelodani pred sudom. Odbijanjem da priznaju kako su njihovi klijenti žrtve sajber kriminala, iz straha da ne izgube korak s konkurencijom, banke posredno potpomažu delovanje kriminalaca.

Naravno, banke imaju problem: njihovi klijenti su najranjiviji deo umreženog finansijskog sistema. Provaljivanje u kompjuterske sisteme najvećih štedno-kreditnih i investicionih banaka danas je izazov čak i za najbolje hakere. Međutim, upadi u kompjutere većine klijenata i potom posmatranje kako pristupaju svojim računima i, štaviše, poigravanje novcem na tim računima, prava je dečja igra za svakog hakera (ili hakerku, mada je njih znatno manje) koji nešto vredi. Kako da unapredite onlajn navike svojih klijenata, kada je velika privlačnost tzv. internet bankarstva (kao što je slučaj s velikim delom naše aktivnosti na Mreži) tako pogodna? Budući da su tako velika gnjavaža, složene bezbednosne mere za pristup njihovim računima generalno idu ljudima na živce.

Banke vole da ćute o razmerama prevare, delom zbog konkurencije, a delom zato što ne žele da njihovi klijenti počnu da zahtevaju povratak na stari način poslovanja. Elektronsko bankarstvo štedi im ogromne sume novca, zato što sve one radnje koje su inače bile posao filijala i njihovog osoblja sad obavlja klijent. Da nekim slučajem svi odbijemo da regulišemo svoje finansije putem interneta, banke bi bile primorane da ponovo uvedu razgranatu mrežu filijala posredstvom kojih bi nas opsluživale. To bi stajalo strašno mnogo novca, a banke, kao što sada znamo, troše sve što imaju, skupa s milijardama gotovine poreskih obveznika, na nečuvena spekulativna ulaganja i nepristojno naduvane bonuse.

Zato je detektiv Doson bio primoran da deliće slagalice sastavlja polako, uz vrlo ograničenu pomoć bankarske bratije. U

prilog mu je, međutim, išla činjenica da je Fred Braun napravio dve značajne greške u konstruisanju svoje prevarantske mreže: naime, iako je njegov *bankfraud@yahoogroups.com* bio registrovan na američki Yahoo!, imejl adresa povezana s njim bila je *yahoo.co.uk*. Pošto je to ime britanskog domena, Doson je uspeo da izdejstvuje sudski nalog i tako odmah dobio materijal od Yahoo!-a. Sa Safemail nalogom je već imao manje sreće. Morao je da zamoli britanski sud da od izraelskog suda zatraži da mu Safemail odobri pristup šifrovanom nalogu Freda Brauna. To se razvlačilo mesecima, a sudovi su ga sve to vreme pritiskali da advokatima odbrane otkrije dokaze kojima raspolaže, kako bi se proces ubrzao.

Dosonovi šefovi nisu bili zadovoljni: osećao je kako pritisak raste. Nijedna od žrtava zločina koji je istraživao nije bila iz Hambersajda – vlasnici kreditnih kartica poticali su iz celog sveta. Jedan, velečasni Džon, bio je iz Zapadnog Jorkšira, ali to je bilo to. „Ne mogu priuštiti sebi da jedan od mojih najboljih detektiva za ubistva radi na slučaju prevare koji nema nikakve veze s ovom oblašću!", više puta je upozoren Doson. Međutim, nešto u njemu ga je teralo napred. Nije hteo da odustane i, kako bi umirio pretpostavljene, počeo je da radi na ovom slučaju u slobodno vreme, katkada do duboko u noć, dok su mu brojevi poigravali pred očima.

Sad već očajan zbog toga kako je istraga Adevala Taiva počela da mu obuzima život, Doson je zamolio za pomoć regionalnu obaveštajnu službu. Nisu mogli da mu pomognu, ali su mu predložili da se obrati londonskom Odseku za visokotehnološki kriminal i zamoli ih za bilo kakvu informaciju koja bi mu bila od pomoći. Nemamo je, glasio je odgovor, ali zašto se ne obratite Agenciji za krupni organizovani kriminal?

Konačno je Doson kontaktirao sa SOCA u njihovom tajnom operativnom štabu u Londonu, koji liči na nešto iz romana Lena Dejtona, kao što su *Dosije Ipkres* ili *Sahrana u Berlinu*: mesingane pločice s nazivom fiktivne kompanije, a svi se pretvaraju da ne rade za agenciju koju je Toni Bler opisao kao britanski odgovor na FBI (što su mu njeni službenici grdno zamerili).

Doson je zamolio za pomoć u složenom slučaju prevare koji obuhvata tajanstvenog čoveka po imenu Fred Braun. Jedan od glavnih baja iz metropole ga je pozvao i kratko upitao: „Šta znate

o Frediju Braunu?" Najzad, nagoveštavao je njegov ton, ti si samo lokalni pandur iz Hambersajda.

„Ništa", odvratio je detektiv Doson, „osim što ga držim u pritvoru ovde u Skantorpu."

S drugog kraja žice doprlo je ćutanje. „Detektive Dosone, jeste li ikad čuli za nešto što se zove DarkMarket?", nastavio je glas.

„Nisam. Zašto?"

Dosonova riba bila je krupnija nego što je i pomišljao.

Međutim, vest je bila poprilično iznenađenje i za SOCA. Freddybb im je već godinama bio na radaru, ali je istraga DarkMarketa zamrla posle serije hapšenja prethodnog leta. Na pamet im nije padalo da će je u život vratiti pandur iz Skantorpa. Međutim, otkako je grupa ukrajinskih sajber lopova 2001. podigla prvi vebsajt posvećen globalnom zločinu, najveći britanski odsek za onlajn kriminal je nešto naučio – da očekuje neočekivano.

Deo II

4.
Dosijei Odesa

Odesa, Ukrajina, jun 2002.

Došli su daleko sa severa, čak iz Sankt Peterburga i iz Letonije, na Baltičkom moru; jedan delegat stigao je iz Belorusije, zemlje nastale 1990, očigledno živog spomenika komunizmu. Rusi su pristigli u povećoj grupi, a Ukrajina je poslala delegate odasvud, iz Ternopila na zapadu, Kijeva u centralnom delu zemlje, Harkova na severu ili Donjecka na istoku.

Međutim, Prvi svetski kongres kardera (First Worldwide Carders' Conference, FWCC) bio je uistinu internacionalan. Neki učesnici došli su iz Zapadne Evrope, dok su neki drugi doleteli čak iz Persijskog zaliva, Kanade i Južne Amerike. U zvaničnom saopštenju FWCC-a izražena je žalost organizatora zbog toga što delegati iz Australije i Jugoistočne Azije, usled otežanih uslova putovanja, nisu uspeli da dođu.

Od oko četiri stotine molbi, organizatori su pažljivo odabrali četrdesetak delegata. Oni koji su imali sreće da prođu, znali su da će im već sam poziv uveliko podići ugled u zastrašujuće hijerarhijskom svetu onlajn kriminalaca.

Da bi zavarali trag policiji, organizatori su prvobitno objavili da se skup održava na nekoliko luksuznih jahti ukotvljenih na turskoj obali Crnog mora. To je, međutim, bio samo manevar namenjen da odvuče pažnju. Najzad, gde bi se drugde mogao održati prvi svetski kongres sajber kriminalaca sem u Odesi – ukrajinskom legendarnom gradu lupeža?

Primenjujući svoje oprobane metode, i ruski carevi i Staljin i Hitler pokušali su da ukrote ovu divlju zver, ali niko od njih nije uspeo da slomi najdugovečnije zločinačko bratstvo Istočne Evrope. „Ako ne znate za gangstere Odese i njihov život", napisao je

jedan hroničar o svom rodnom gradu, „istorija ovog grada vam je jednostavno nerazumljiva."

Neumoljivi gangsterski kapitalizam, koji je usledio posle kolapsa komunizma devedesetih godina prošlog veka, predstavljao je istinski šok za najveći deo Evrope. Međutim, Odesa je znala šta sledi. Njenim žiteljima nije bilo druge do da prihvate novu eru – što su, moglo bi se reći, uradili s izvesnim poletom. Crvene zvezde su preko noći zamenjene crvenim svetlima. Musave kockarnice nicale su kao pečurke posle kiše na Primorskom bulevaru, a nedugo posle 1989. restorani i saune postali su poprišta prežderavanja i krvoprolića.

Podalje od centra, u stambenim blokovima, droga je postala valuta izbora. Mlađarija praznih džepova navukla se na *boltušku*, amfetaminsku mešavinu kućne izrade koja ih je ostavljala u ožiljcima, s psihičkim oštećenjima ili mrtve.

Revolveraši i klanovi izdaleka, čak iz Čečenije i Moskve, borili su se s lokalcima tipa Robina Huda za prevlast u gradu – naime, iako je Odesa u teoriji bila deo nove nezavisne Ukrajine, u celosti je pripadala ruskom govornom području i, što je još važnije, bila je jedina luka koja se ne zamrzava i kadra je da prihvati celokupan ruski izvoz gasa i nafte.

Hiperinflacija i nacionalizam uništili su vrednost rublje, karbovanjeca, hrivnje i svega ostalog za šta je vlada u datom trenutku tvrdila da je „pravi" novac. Jedinu stvarnu stabilnost pružao je jenkijevski dolar.

Većini običnih ljudi, Odesa je 1990. značila dve stvari: opstanak i dolare. Niko nije mario niti se mrštio zbog toga kako ste uspevali prvo i namicali drugo. Štaviše, poštovali su one koji su postizali bilo šta od toga, premda iznenadno bogatstvo nije bilo nikakva garancija dugovečnosti.

U takvoj atmosferi, ko je mogao zameriti trinaestogodišnjem Dimitriju Golubovu što je prodavao papire za registraciju vozila i vozačke dozvole s falsifikovanim potpisom direktora Opštinskog odseka za saobraćaj? Ako su poslovni ljudi bili spremni da za to plate, valjda trgovina stvarno nečemu vredi?

To je još uvek bilo u tipičnom fazonu Odese. Međutim, mladi Dimitri posedovao je nešto što ga je smeštalo u drugačiji svet od tradicionalnog gradskog gangsteraja koji se bavio reketiranjem, bordelima, naftom i kavijarom. Umesto da nosi nož, umeo je da s ulice siđe u zadimljene mračne podrume u kojima su

kompjuterske igrice poput *Street Fightera*, *Packmana* i onog ruskog klasika, *Tetrisa*, neumorno pretvarale mozak tinejdžera u sutlijaš. U ovoj podzemnoj kulturi, jedina svetlost dopirala je od neonskih oblika prigušenih boja i treperavih PC monitora. Cigarete i koka-kola bili su u toj meri sveprisutni, da je izgledalo kao da su jedina košer ishrana koju odobrava neki prastari nepisani zakon gikova.

Dimitri je voleo igrice koliko i svi ostali, mada mu je bilo draže da istražuje svet iz udobnosti odeskih internet-kafea. Međutim, mladi Golubov nije uživao samo u surfovanju po sajtovima dalekih zemalja nego je želeo i da prodre u njih i istraži njihovu unutrašnjost.

Kad je imao šesnaest godina, 1999, Visa i MasterCard blokirali su upotrebu svojih kartica na vebsajtovima registrovanim na bivši Sovjetski Savez. Kad su ruske internet kompanije predale fakture ovim kreditnim gigantima, ignorisali su ih. Međutim, Golubov i njegove kolege pioniri ubrzo su shvatili da, ako nekako uspeš da izvučeš informacije sadržane na kreditnoj kartici i reprodukuješ ih, tada možeš da upotrebiš podatke za skidanje gotovine s bankomata ili kupovinu robe putem interneta, a da ih onda pošalješ trećem licu negde drugde u svetu. Jedna opcija bilo je kopiranje informacija sa same kreditne kartice, premda je to isprva podrazumevalo naporan i stoga u celosti nezadovoljavajući čin konvencionalne pljačke. Neuporedivo bolje bilo je da se prosto domogneš informacije pohranjene u zlatnim rudnicima banki podataka kompanije!

A čak i ako nisu hteli da isporučuju robu u bivši Sovjetski Savez, neki američki vebsajtovi su je rado slali u mesta poput Ujedinjenih Arapskih Emirata ili Kipra, dveju zemalja koje su vrlo brzo postale omiljene destinacije nove ruske bogate elite. Bio je to jedan od prvih istinski globalizovanih zločina. Rus je u Ukrajini krao novac od američke banke, a isplata se vršila u Dubaiju – pri čemu čitava transakcija nije trajala duže od deset minuta!

Drugi veliki prodor koji je oblikovao novu profesiju „kardinga" bio je uređaj za skiming (skimming).[10] „Skimeri" su mašine koje čitaju i skladište magnetnu traku na kreditnoj kartici. Ima ih u više oblika i veličina. Neki su mali pravougaonici koji se mogu pričvrstiti na bankomat i, kad automat čita karticu klijenta,

10 Eng. *skim* – obrati (voće), skinuti kajmak (u stvarnom i u prenosnom značenju), kliziti po površini i sl. (Prim. prev.)

čita je i „skimer". Ostali izgledaju identično kao uređaji kroz koje će vam konobar u restoranu ili blagajnik na benzinskoj pumpi provući karticu kada plaćate. I na bankomatu i na nevaljalom uređaju za provlačenje kartice se, vrlo moguće, negde nalazi skrivena majušna kamera koja snima klijenta dok unosi svoj PIN (napomena: *uvek* pokrijte tastaturu kad ukucavate PIN).

Ovi uređaji se nazivaju „skimeri" samo ako se koriste u nezakonite svrhe, inače su po funkciji identični onima koji se nalaze u redovnoj prodaji. Neki „skimeri" se komercijalno proizvode i kriminalci ih tako nabavljaju, a neki su kućne izrade. „Skimer" je bio karderski ekvivalent parnoj mašini Džejmsa Vata na početku industrijske revolucije. Tokom naredne decenije, ogromna većina brojeva kreditnih kartica i PIN kodova („dumps" (dampovi) i „wholes", kako se žargonski nazivaju) koje su upotrebili prevaranti „skliznula" je na taj način sa bankomata i biznisa širom sveta.

Kao talentovani haker, Dimitri je takođe vrlo brzo uočio i da su bezbednosni sistemi koje razvija zajednica elektronske trgovine (e-commerce), tada još u povoju, primitivni i da ih je lako provaliti. Nije poznato koliki je uspeh imao u početku. Dima je voleo da priča naokolo kako je zlatni standard dolarskog milionera dosegao pre no što je proslavio sedamnaesti rođendan. Ali ne zaboravite jedno: laži su najčešća valuta na internetu, a neki od njegovih sajber pajtaša kazuju drugačiju priču.

„Bio je gramziv, prevrtljiv i oduvek ga je privlačio kriminalni milje", blogovao je drugi haker iz Odese. „Međutim, imidž uspešnog milionera bio je veoma daleko od stvarnosti."

Dimitri je tada nestao, zajedno s nekim svojim drskijim šemama za zarađivanje. Nekoliko meseci kasnije pojavio se ponovo, ovog puta anonimno, pod imenom Script, veličanstveno vešt stvor koji je ushićeno provodio vreme na dva nova vebsajta, *carder.org* i *carder.ru*. Zapravo, bili su tek nešto više od diskusionih foruma na kojima su ruski hakeri razmenjivali misli o tome kako da se domognu trilijardi dolara, funti, jena i evra zaključanih iza kreditnih kartica. Jedan od prvobitnih članova ovih sajtova seća ih se kao „nesređenih, nestabilnih" i krajnje „nezadovoljavajućih".

Script je, međutim, dugo i napregnuto razmišljao. Ako postoje vebsajtovi za sve druge vrste trgovine, zašto ne napraviti i jedan namenjen onoj koja je tek u začetku – trgovini ukradenim brojevima kreditnih kartica, bankovnih računa i ostalim dragocenim podacima? Imao je snažan motiv za želju da uspostavi takvo

prisustvo na Mreži. Naime, Script beše počeo da nagomilava velike količine tih podataka, koje nije imao vremena niti resursa da eksploatiše. Hteo je da pretvori sve svoje brojeve u gotov novac. Hteo je da ih proda.

Trenutak je bio savršeno odabran. U prethodnih pet godina, internet je postao središte pomamnog razvoja komercijalne aktivnosti. Bilo je to nešto što niko nije u potpunosti predvideo, budući da su njeni začetnici zamislili Mrežu kao instrument za unapređenje i ubrzanje komunikacije, poprište razmene ideja i tračeva.

Amazon, eBay, *lastminute.com* i ostali prvi drmatori sajber preduzetništva pali su kao s neba. Međutim, njihov uspeh nije prošao neprimećeno. Hiljade i hiljade ljudi oprobale su se u postavljanju vebsajtova. Kako je to bio jedan od onih istorijskih trenutaka koji se dešavaju jednom u generaciji, kad ljudska pohlepa i mašta koincidiraju, nije prošlo dugo a banke i investitori skloni riziku ubedili su sebe da e-trgovina garantuje brzo bogaćenje. Počeli su da ulažu novac u te kompanije, od kojih su veliku većinu činili u suštini bezvredni poslovni subjekti, uprkos tome što su kapitalizovane milionima, ako ne i desetinama miliona dolara. Tako je nastao prvi veliki mehur globalizovanog doba; kako je primereno to što su ga činile haj-tek deonice.

Međutim, iako su dot.com kompanije mahom bile komercijalna Potemkinova sela, firme već uhodane u stvarnom svetu zaključile su da će im biti vrlo korisno da deo svog poslovanja obavljaju na Mreži.

Kao što smo već rekli, banke su se tu brzo snašle jer su shvatile da, ako uspeju da ubede svoje klijente da uplate vrše i svojim računima upravljaju putem interneta, neće morati da plaćaju službenike da obavljaju taj posao. Bilo je skoro sigurno da će klijenti koji se dobro snalaze na Mreži više voleti da imaju neposrednu kontrolu nad svojim finansijama kakvu omogućava internet bankarstvo.

U to vreme su Gospodari svemira, nova klasa finansijskih kapitalista,[11] zbacivali okove koji su u prošlosti ograničavali njihovu spekulativnu aktivnost na derivativnim tržištima. U suštini,

11 Tom Volf je u svojoj knjizi *Lomača taštine* (*The Bonfire of Vanities*, 1987) nazvao ambiciozne karijeriste sa Volstrita „Gospodarima svemira" (Masters of the Universe). Isti izraz upotrebljen je i u istoimenom filmu iz 1990. (Prim. prev.)

političari u Vašingtonu i Londonu izdali su im dozvolu za kockanje (dobar primer je bum dot.com kompanija) i, kako je cena hartija od vrednosti koje su vredele veoma malo skočila nebu pod oblake, novac se pozajmljivao na osnovu navodne vrednosti tih hartija. Zapadni svet se čitavu deceniju baškario u jeftinom kreditu. Ages of Empire i kapital preobrazili su se u Doba plastike.

Sredinom devedesetih, dugovanja na personalnim kreditnim karticama u četiri najveća korisnika plastike – SAD, Velikoj Britaniji, Japanu i Kanadi – počela su da narastaju ludačkim tempom. Za deset godina koje su usledile od 1997, broj kartica u opticaju u svetu porastao je sa 1,3 milijarde na 3 milijarde, a prosečna pojedinačna zaduženost među najgore navučenim korisnicima, Amerikancima, udvostručila se sa pet hiljada na 10 hiljada dolara. Banke su naprosto obožavale ovu novootkrivenu ljubav prema kreditnim karticama, jer su u vreme kad su kamate bile takoreći ravne nuli, ipak veselo naplaćivale interes koji se kretao od pet do 30 procenata. Čelnik britanskog Barclaycarda priznao je pred parlamentarnom komisijom kako „ne uzima pozajmice preko kreditnih kartica, zato što su preskupe".

Ostali delovi planete nisu se tako lako dali ugurati u taj kalup od plastike. Zapadna Evropa se tradicionalno klonila gusarske privrede koja je tako omađijala Ameriku i Britaniju. Posledica toga bila je da je broj vlasnika kreditnih kartica bio mnogo manji, jednako kao i nivo lične zaduženosti. U Istočnoj Evropi nije bilo dovoljno kapitala u posedu stanovništva, niti bezbedne bankarske industrije koja bi izdavala kreditne kartice. U nekadašnjem komunističkom svetu plastika je bila retkost, nova kancelarijska igračka za Nove Ruse – onaj majušni procenat populacije koji je zgrnuo basnoslovno bogatstvo tako što je u razdoblju tranzicije iz komunizma u kapitalizam opljačkao svoju državu i zemljake.

Međutim, u kasino-ekonomiji devedesetih i dvehiljaditih, plastika je bila nešto najbliže štampanju novca što su finansijske institucije ikada smislile i žurno su iskopavale tu zlatnu žilu kapitala. Na adrese u zapadnom svetu svakodnevno su slate tone letaka kojima su nagovarali ljude da poruče kreditne kartice ili zamene postojeći dug za novi račun, na kom im se šest meseci neće zaračunavati kamata. Marljiviji klijenti bili su u stanju da za tri ili četiri godine obezbede sebi beskamatni kredit, tako što su prebacivali svoje veliko zaduženje s jedne kartice na drugu, dok su banke još grozničavije nastojale da obezbede sebi nove klijente.

Toliko kartica. Toliko novca kojim se možeš igrati. Pošto su se Mrežom doslovno prosipali debeli elektronski svežnjevi novčanica, možda ne iznenađuje što je to počelo da privlači pažnju sajber ljudi s Istoka, koji su oskudevali u novcu ali su zato cepteli od tehničke ingenioznosti. Jedan od njih bio je i Script, osamnaestogodišnji Dimitri Golubov iz Odese.

Tako je rođen CarderPlanet.

5.
Carderplanet

Na ekranu lagano bledi pitanje, ispisano treperavim fontom Ratova zvezda:

TRAŽIŠ PROFESIONALNO REŠENJE?

Snimak zumira na Zemlju koja se okreće sve brže i potom eksplodira u metalni psihodelični obrazac, a sve to propraćeno je agresivnom tačkom elektro-densa i nizom poruka:

OTKRIJ MOĆ TEHNOLOGIJE
DOSADILA TI JE SVAKODNEVNA RUTINA?
ŽELIŠ DA PROMENIŠ STIL ŽIVOTA?
POSTANI JEDAN OD NAS!
DAMPOVI – KREDITNE KARTICE
MOGU TE UČINITI BOGATIM!

Zatim se ekran lagano zacrni, pre no što se pojave još tri poruke, naglašene promuklim vojnim dobošem:

TIM NA KOJI SE MOŽEŠ OSLONITI
BUM!
SVE ŠTO TI JE POTREBNO ZA BIZNIS
BUM!
KARDERPLANET JE NEOPHODAN
BUM!

Godinu dana nakon što je osnovan CarderPlanet (2001), Script je pozvao svoje prijatelje hakere na Prvi svetski kongres kardera u Odesi – prvi ikad održan svetski skup sajber kriminalaca – da proslave svetsku uspešnost vebsajta. Ta grupa se mogla podičiti istom neverovatnom sajber sposobnošću kao Hakerska republika,

tajna grupa kojoj je, pod nadimkom Osa, pripadala Lizbet Salander, junakinja bestselera Stiga Lašona *Muškarci koji mrze žene*.

Međutim, u vezi sa Scriptom i njegovim drugovima nije bilo ničega fiktivnog. CarderPlanet je bio stvaran.

6.
Porodična stvar

Prvi svetski kongres kardera proslavio je prvi rođendan CarderPlaneta. Bilo je jedinstveno i nezaboravno. Do 2002. Odesa se smirila: čak su bili prisutni i znaci normalnosti. Njen legendarni Bulevar Deribasovska vrveo je od uličnih prodavaca, dućana i mondenskih restorana. Okruženi detelinom sa četiri lista i galskim natpisima Mik O'Nila (Mick O'Neill's), jednog od prvih lažnih irskih pabova u postkomunističkoj Ukrajini, jezgro vrhunskih ukrajinskih hakera, poznato kao Porodica, raspravljalo je o ciljevima kongresa. Među njima su bili glavni igrači, poput Auditora, Raydena i Bigbyera, kao i duhovne vođe skupa: Boa, vrhunski stručnjak za komunikacije i bezbednost s karakterističnom belom bradom, i energični mada pomalo balavi Script.

Naredna tri dana pili su i pevali na nekoliko različitih lokacija u gradu, ali pre svega su razgovarali o dugoročnom i kratkoročnom razvoju svog novog vebsajta, CarderPlanet, koji je već menjao prirodu sajber kriminala širom sveta.

Opšte diskusije održavale su se u hotelu „Odesa", koji je u to vreme bio najskuplji u gradu. Visoka zgrada, inače dobar primer *ružnog postkomunističkog* šika, barem se nalazila na pristaništu, odmah preko puta Potemkinovih stepenica, ovekovečenih u Ajzenštajnovoj *Krstarici Potemkin*, remek-delu ranog sovjetskog filma. Teme u kojima su uzeli učešća svi delegati u „Odesi" obuhvatale su potrebu za ovladavanjem tehničkim pojedinostima manje upotrebljavanih kreditnih kartica kao što su JCB i Diners, za koje su smatrali da su zanemarene u korist unosnijih Visa i MasterCard franšiza. Takođe je dogovoreno da se razviju ili ojačaju nove mreže ljudi koji bi mogli da „unovčavaju" ukradene kreditne kartice u udaljenim oblastima kao što su Južna Amerika, Okeanija i Afrika. Najzad, neko je morao da se poduhvati i konkretne nezakonite transakcije u vidu skidanja novca s bankomata –

poveravanje tog zadatka spoljnim saradnicima bilo je krajnje jednostavno rešenje.

One tajnije diskusije, kojima je prisustvovalo samo petnaestak vodećih „kardera", održavale su se u malom musavom restoranu na morskoj obali. Cilj ove grupe bio je da ubedi delegate da uspostave sopstvene regionalne mreže CarderPlanet franšiza, kako bi vlasnici sajta nastavili da zarađuju novac, ali uz manje truda.

Kad je sastanak počeo, jedan manje poznat delegat dao je neupadljivi znak Boi. Ovaj je obavio elektronski pregled restorana i ustanovio da su u prostoriji aktivne skrivene video-kamere i uređaji za digitalno snimanje. Po svoj prilici, nadzirala ih je ukrajinska tajna policija SBU (Služba bezbednosti Ukrajine). A ako je SBU nadgledala skup, isto je moralo važiti i za ruski KGB, koji je u to vreme imao nad SBU obaveštajni ekvivalent *droit de seigneur*, pravu gospodara – pravo preuzimanja podataka pre no što ih onaj koji ih je pribavio uopšte i pogleda.

Porodica, Politbiro ili Kupola CarderPlaneta, nije se naročito plašila američkih i evropskih obaveštajnih i policijskih operacija. KGB je, međutim, bio nešto drugo, i nije bilo slučajno što je najvažnija rezolucija kongresa upozoravala na neprijateljske aktivnosti u Rusiji i Ukrajini. „Još jednom naglašavamo da su apsolutno nedopustive bilo kakve akcije u odnosu na domaće obračunske sisteme, banke ili finansijske institucije", strogo je podsećala. Da su se ruski sajber kriminalci okrenuli ruskim bankama ili firmama, ceo projekat bio bi zatvoren u roku od pet minuta.

Umesto toga, CarderPlanet ispostavio se kao izdržljiviji. Vebsajt je postojao skoro četiri godine. Ne preterujem kad kažem da su njegovi tvorci odgovorni za pojavu i konsolidovanje potpuno novog metoda uključivanja u krupnu kriminalnu aktivnost: prevare koja se može izvesti u velikim razmerama, a uz minimalne resurse i rizik.

Prvenstvena uloga CarderPlaneta (koju su kasnije usvojili mnogi sajtovi osnovani po uzoru na taj) bila je da deluje kao pijaca ukradenih podataka – brojeva i PIN-ova kreditnih kartica, bankovnih računa i lažnih papira. Sve dotad, razmena takvih informacija generalno se odvijala putem nimalo jednostavnih transakcija između dveju osoba putem ICQ-a i IRC-a (dva mesindžera omiljena među hakerima).

Izvršioci sajber kriminala – takozvani karderi, spameri, skimeri i tvorci virusa – već su ličili na sasvim drugačiju vrstu od

kriminalaca vezanih za tradicionalne mafijaške strukture. Script ih je u intervjuu za sajt *Haker* (*Хакер.ru*), veliki hroničar ruskog sajber podzemlja, nazvao „vukovima samotnjacima". „Ne drže se u grupama i ne obrazuju sopstvene zasebne mreže; svak radi sam i radi za sebe."

Rusi nisu bili jedini hakeri koji su razvijali tehnike sajber kriminala, ali CarderPlanet im je dao strukturu, koja je dotad bila nepouzdana, omogućavajući tim vukovima samotnjacima da se, onda kad im to odgovara, udružuju u privremene čopore kako bi počinili zločin (ili običan nestašluk), posle čega ponovo ispare u pustu sajber divljinu, briljantno kamuflirani u klikovima i brujanjem ispunjenom okruženju Mreže, odupirući se svim pokušajima da se utvrdi ko bi uopšte mogli biti.

Članovi CarderPlaneta su vrlo brzo počeli da obožavaju taj sajt. „Moraš da razumeš", rekao je bivši *konsiljere* iz unutrašnjeg kruga sajta, „CarderPlanet nije bio samo izvor informacija. Ljudi su živeli na njemu – zvali smo ga prosto Planeta, kao da nam je rođena kuća."

Premda su prevare, spaming i drugi oblici elektronskih nezakonitih radnji igrali veoma važnu ulogu, to ni slučajno nisu bile jedine aktivnosti koje su privlačile ljude s ruskog govornog područja da se spuste na Planetu i nastane na njoj. Prosečan korisnik bio je zaluđen elektronikom, informatikom, igricama, mrežnim sistemima i hakovanjem kao sportom.

To nisu bili obični kriminalci koji su poistovećivali CarderPlanet sa kanalom putem kojeg bi se mogli baviti svojim zanatom. Umesto toga, stvorili su zajednicu, mahom mušku, ljudi u tinejdžerskim i ranim dvadesetim godinama koji su se mučili da se snađu u haotičnom, nemilosrdnom istorijskom trenutku i koji su posedovali jedinstvene sposobnosti. U Odesi su svi bili primorani da pribegavaju određenim nezakonitim postupcima i to je bilo sasvim normalno. Međutim, većina je bila prirodno ograničena mestom boravka. Planetaši su se naoružali logikom ljudi rešenih da opstanu u političkom i privrednom metežu Odese, i preslikali te bihevioralne obrasce u sajber svemir. Oni nisu bili rođene ubice već ljudi s urođenim nagonom za opstanak.

Novi sajt je bio podeljen u kategorije posvećene konkretnom aspektu internet kriminala ili hakovanja. Kad se prvi put ulogovao na CarderPlanet, jedan mladi haker iz Odese bio je zapanjen. „Kunem se da je to isto morao osetiti Alibaba kad je prvi put

otvorio pećinu i ugledao sve ono silno blago u njoj. Svaka oblast bila je krcata informacijama, koje si mogao da iskoristiš da se obogatiš kao Krez, a da pri tom nijednom ne ustaneš od kompjutera!"

Prve godine sajt su počele da istražuju stotine i stotine hakera s ruskog govornog područja, privučene zabavnom grafikom i efikasnom organizacijom. Vizuelni logo CarderPlaneta bio je lik sa cigarom i iskrom u oku – pljunuti Fleš Hari, drski probisvet koga je glumac Džordž Kol tumačio u britanskom posleratnom komičnom klasiku *Devojke iz Sent Trinijana* (*The Belles of St Trinian's*).

„Za bezazlene klince iz provincije, poput mene, koji su u najboljem slučaju mogli očekivati zaradu od stotinak dolara mesečno", nastavio je mladi haker iz Odese, „finansijsko obećanje ovog nepoznatog jezika – koji je obuhvatao reči kao što su dampovi, dropovi, žice, COB-ovi – zvučalo je opčinjavajuće."

Sajt nije bio otvoren za sve i svakog. Da bi pristupio njegovim zatvorenim delovima, morao si da se učaniš, što je značilo da će te administratori dobro proveriti. Pored Scripta, u prvoj godini aktivnosti CP-a, ovu povlašćenu ulogu imala su još četvorica, među kojima i Boa, najuticajniji Scriptov saradnik.

Administratori su, između ostalog, odlučivali kome će članstvo biti odobreno, a kome neće. Te bezbednosne mere su pre svega bile osmišljene da odbiju interesovanje kriminalističkih službi i obaveštajnih agencija iz celog sveta. Tajna služba SAD i britanski MI6 bili su dobro upoznati s prethodnicima CP-a, sajtovima *carder.org* i *carder.ru*. Script je bio rešio da im ovog puta ne dopusti da mu priđu. Bio je ubeđen da ukrajinska policija ne predstavlja nikakvu naročitu pretnju sajtu. „Potpuno su neopremljeni, ne poseduju potreban kadar niti resurse", tvrdio je. „U ukrajinskim službama nema nikog ko tečno govori engleski i, u svakom slučaju, teško da kapiraju išta od ovoga. Prema tome, sve i da se domogu neke informacije od 'neprijatelja', tj. od nas, neće umeti da je pročitaju (niti dobijaju finansijska sredstva za to), tako da, u suštini, nemaju šta ni da pročitaju."

Međutim, ruske kolege iz Odseka R Ministarstva unutrašnjih poslova, koji je docnije reorganizovan i preimenovan u Odsek K, sa zadatkom da se bavi svim vidovima sajber kriminala, bile su upornije od ukrajinske policije. Ruska Tajna policija prodrla je na CarderPlanet i ugrozila ga skoro čim je podignut. Međutim, kao

što je istakao beloruski karder s nadimkom Police Dog (Policijski Pas): „Ako ne prljamo vlastito dvorište, tada naši lokalni panduri i obaveštajne službe neće imati problema s nama." Zašto bi KGB trošio svoje resurse na istraživanje mreža koje „deru" američke i evropske kreditne kartice? Potpuni gubitak vremena. Stoga se Moskva privremeno zadovoljavala time da posmatra i skuplja informacije. Tačno su znali ko je ko u karderskoj zajednici Odese.

Ironično – s obzirom na to da su se CarderPlanet i sajber kriminalci dičili sasvim drugačijim društvenim, kulturnim i psihološkim profilom u odnosu na tradicionalne sindikate zločina – Script i njegovi saradnici su ipak odlučili da svoju člansku strukturu obeleže terminologijom pozajmljenom od sicilijanske mafije. Karderi su kasnije smatrali da nije bilo pametno upotrebiti tako očigledno kriminalnu metaforu, mada je u tim prvim danima način izražavanja nagoveštavao i Scriptov specifični psihološki profil i njegovu buduću ambiciju da predvodi moćni društveni pokret.

Članovi najviši po rangu (nikad više od njih šest) pripadali su „Porodici", čiji su najviši predstavnici ili administratori dobijali počasnu titulu „kuma". Tek kad ove starešine Porodice odobre nekom učlanjenje na CarderPlanet, član je mogao da istražuje raznorazne delove sajta. U jednom delu, na primer, mogao je da razgleda čitavu zbirku virusa na prodaju, koje je kasnije mogao upotrebiti za specifičan napad na ostale korisnike kompjutera. Tvorci virusa nudili su i da za određeni iznos napišu prilagođeni malver, kadar da se infiltrira u izvesne sisteme ili programe.

Najveći deo aktivnosti odvijao se na forumu Cardera, na kom se vršila kupoprodaja ukradenih podataka s kreditnih kartica i bankovnih računa. „U svom poslu", objašnjavao je Script, „karder se može specijalizovati za jednu ili više oblasti kardinga. Međutim, ne postoji niko ko radi baš sve. Pre ili kasnije, tom karderu će zatrebati usluge drugih. Zato i ima mesta za mreže i grupe – ljudi razmenjuju brojeve i informacije. To mogu biti bankovni računi, sa svim informacijama o vlasnicima kartica, ponekad čak i s podacima iz pasoša. Karderi mogu ujedno biti i hakeri, budući da ponekad ne možeš da dobiješ neophodne informacije (a da ne platiš za njih) sem ako ne provališ na server."

U drugom odeljku mogao si da kupiš pasoš neke zapadne zemlje ili, recimo, američku vozačku dozvolu. Falsifikovani papiri su

u većini slučajeva bili izuzetno kvalitetni. Međutim, kako da ti, kao kupac, budeš siguran u kvalitet tih lažnjaka? Štaviše, kako da budeš siguran da te prodavac neće odrati? Najzad, već znaš da je taj od koga kupuješ kriminalac! Na internetu su još tad uveliko postojali „ripperi" („deratori") – kriminalci koji pljačkaju kriminalce.

To je bila najjača karta CarderPlaneta. Članovi Porodice pratili su sve dolaske i odlaske. Posle uvođenja sistema provere, dodatno su pojačali bezbednost tako što su počeli da naplaćuju pristup u članstvo, kako bi odbili smutljivce. U početku su imali „veliki priliv amatera, koji su samo pravili nepotrebnu gužvu na forumu", ali još je štetnije bilo prisustvo deratora, „koji pružaju usluge lošeg kvaliteta ili uzimaju novac a ne isporučuju dogovorene usluge".

Međutim, CarderPlanet nije bio samo robna kuća za sajber lopove, budući da je sistem provere omogućavao administratorima da jemče za poslove koji se obavljaju preko njihovog sajta. U zamenu za to, dobijali su laskave pohvale, gotovinu i mnogo veće i efikasnije tržište za vlastite proizvode, a sve to jednim udarcem.

Iako pravi pravcati haker, Script je bio neobičan utoliko što se pre svega rukovodio željom da zaradi. Mada mlad, odlično je procenio okeane gotovine u kojima je plivao zapadni svet, a pogotovo Amerika. Profit je neosporno moćna sila, ali kreativni genije koji je stajao iza CarderPlaneta nije bio Script već njegov stariji saradnik Boa, kome je novac bio u drugom planu.

Boa je bio sasvim drugačija ličnost od ostalih stanovnika Planete. Već u kasnim tridesetima kad je Script napravio Planetu, imao je dobrih dvadeset godina više od većine svojih kolega i neizmerno mnogo više životnog iskustva.

Osamdesetih godina prošlog veka, dok je još postojao Sovjetski Savez, Boa se pokazao kao talentovani student elektronike i stekao je dve univerzitetske diplome. Usput se naročito zainteresovao za svet radio-amatera. U to vreme, to je bio prilično nezgodan hobi zato što se sovjetska obaveštajna služba (a u slučaju kratkotalasnog radija, *vojna* obaveštajna služba) grdno trudila da zadrži kontrolu nad svim komunikacijama koje su vodile u zemlju i iz nje.

Boa je bio strahovito popularan, a njegova prijaznost je umela da za tren oka preraste u harizmatičnost. Bez obzira na to što su neki prijatelji pretpostavljali da sarađuje s odsekom za

signale[12] pri vojnoj obaveštajnoj službi, postao je uzor radio-amaterskom bratstvu celog sveta koje, kao što možete i zamisliti, sadrži i poveći procenat stidljivih gikova.

Boa je stekao svetski ugled time što je postao prvi radio-amater koji je emitovao iz zabranjene vojne zone vijetnamskih ostrva Spratli, propativši to još više zadivljujućim dostignućem: slanjem prvih radio-amaterskih signala svih vremena iz Severne Koreje. Zbog tog podviga odavali su mu počast u celom svetu, od Amerike preko Evrope do Australije, i na svim skupovima radio-amatera devedesetih godina privlačio je prave horde fanova. Zgodan i izuzetno elokventan, ubirao je instinktivne simpatije ljudi i svi su želeli da mu budu prijatelji.

Boa je na CarderPlanet naišao dok je surfovao Mrežom u jesen 1999, a njihov preduzetni, mada pomalo haotičan duh, smesta je ostavio utisak na njega. U to vreme je živeo na Malti i već je posedovao globalno uspešnu firmu koja se bavila prodajom skupe opreme za nadziranje, kontra-nadziranje i antiterorističke tehnologije političarima i poslovnim ljudima u više od šezdeset država širom sveta.

Svestan Boinog profesionalnog iskustva i organizatorskih sposobnosti, Script ga je posle nekoliko meseci pozvao da se pridruži „Porodici". Impresioniran Scriptovom preduzimljivošću i energijom posle prve posete sajtu početkom 2002, Boa je pristao da se priključi CarderPlanetu. „Kad nam se Boa pridružio, Planeta je živnula", priseća se jedan od mladaca koji su prešli na Planetu. „Bio je zaslužan za fensi dizajn, a uveo je i veliki broj novih odeljaka. Pročuo se među nama."

U isto vreme, Boa se dogovorio sa Scriptom da će napraviti još jedan sajt, Boa Factory, čije bi aktivnosti dopunjavale rad CarderPlaneta i isticale neke druge sektore tog posla – Boa Factory je, između ostalog, bio poznat kao specijalista za proizvodnju falsifikovanih pasoša i ličnih karata, ali i po velikoprodaji kloniranih kreditnih kartica i dampova. Dok je Boa Factory bio isključivo poslovni sajt, CarderPlanet je naglasak stavljao na društveni aspekt podzemlja, kao mesto gde se individualni karderi mogu sretati, četovati, kupovati i prodavati na Mreži.

12 Deo obaveštajne službe koji informacije prikuplja putem presretanja signala, bilo između ljudi ili iz elektronskih signala koji nisu direktno uključeni u komunikaciju, ili iz kombinacije to dvoje. (Prim. prev.)

Boa Factory je razvio revolucionarnu alatku, koju je docnije usvojio i CarderPlanet, a koja je omogućila porast sajber kriminala u industrijskim razmerama. Najveći izazov s kojim su se sajber lopovi suočavali ležao je u spoznaji da je osoba s kojom posluju takođe kriminalac i da joj *ipso facto*[13] nije verovati. Kako bi rešio taj problem, Boa je osmislio sistem uslovnog dogovora i depozita, u početku poznat kao Garantni servis. Prodavac je mogao dostaviti nadležnom službeniku uzorak svoje robe (desetak brojeva i PIN-ova kreditnih kartica), dok bi mu potencijalni kupac istovremeno poslao novac. Službenik je zatim isprobavao robu i, ako donosi gotovinu kao što je i obećano, prosledio bi novac prodavcu, a dampove i PIN-ove kupcu. Ispostavilo se da je ova jednostavna zamisao pravi dodir genija. Trgovina je otad bila zaštićena i doživela je pravi bum.

Okupljanje Porodice na Prvom svetskom kongresu kardera u leto 2002. bila je Boina zamisao. Stoga, kad su njegove pozivnice da posete Odesu pale na elektronske otirače širom nekadašnjeg Sovjetskog Saveza, primaoci su bili više nego spremni da sednu u avion i upute se na jug (premda su trošak za kartu skoro sigurno nakačili na nečiju tuđu kreditnu karticu). Bi li katolik propustio priliku da poseti Lurd? Ili musliman šansu da vidi Meku? Dakle, nijedan krimos koji drži do sebe ne bi odbio ponudu da provede nedelju dana u Odesi.

Uoči samog skupa, Script je dao intervju za javnost, kao prvi veliki karder koji je ikad uradio tako nešto. *Хакер.ru* (magazin *Hacker*), koji i dan-danas izlazi, predstavlja bibliju ruskog podzemlja, ali čak su se i njegovi čitaoci šokirali kad su, marta 2002, videli kako Script otkriva tajne Planete. „Šta te je motivisalo da postaneš karder?", pitao je časopis Scripta, istakavši kako je zloglasni ruski Odsek R obrazovan baš zato da lovi kardere i njihovu felu.

Script: Motiviše ih ono što im kazuju njihovo srce i duša. Nauka je dokazala da ljudi koji rizikuju doživljavaju nagli porast nivoa takozvanog hormona sreće. Taj hormon, umnožen izvesnom količinom šuškavih dolarskih novčanica, igra

13 Lat.; samim tim, podrazumeva se, u skladu s tim, samo po sebi i sl. (Prim. prev.)

fundamentalnu, presudnu ulogu u motivisanju nekoga da nastavi da radi u ovoj ne baš sasvim poštenoj industriji.

Hacker: Mirne savesti?

Script: Mirne savesti. Ne samo zato što svako može stornirati svaku transakciju čak i posle dužeg vremena, prosto tako što će poslati banci izjavu u tom smislu, nego i zato što karding i nije baš toliko gnusno zanimanje kao što možda izgleda. Mnogo je manje sramno od pljačke. Mi ne stvaramo nikakve probleme vlasnicima kartica: njima će banka, ako zatraže, vratiti ceo iznos, do poslednjeg novčića. Umesto toga, naša vlada bi trebalo da ima grižu savesti zbog toga što su tinejdžeri tako mladi postali proneveritelji.

Golubov je racionalizovao karderski zanat onako kako to radi većina njih: ceh na kraju uvek plati banka, pa običan svet ne trpi nikakvu štetu. To sentimentalno populističko bulažnjenje vrlo zgodno preskače to da banke troškove ovakvih prevara prenose na svoje klijente, tako da karderi vrlo direktno i negativno utiču na običan svet prema kojem je Script ispoljio navodnu obzirnost.

Ipak, što se tiče toga da vlada ne daje ni pišljivog boba za pojavu velikog broja tinejdžera koji se okreću kriminalu, gotovo da je u pravu. Ukrajina je bila malo više od mafijaške države, a njeni vodeći političari i poslovni ljudi bili su grozan uzor, u koji se Script, ispostavilo se, vešto ugledao.

Postavljen naspram takve pozadine, Script je verovao da će CarderPlanet uspeti da mu obezbedi dovoljna finansijska sredstva da pređe u jaču ligu ukrajinskog biznisa. Ako ništa drugo, zaista je bio ambiciozan.

Šta je moglo da pođe naopako?

7.
Udavljeni udav

Negde u vreme kad je Script u Odesi pokrenuo CarderPlanet, istraživači softverskog giganta Autodesk u San Rafaelu, u Kaliforniji, zaključili su da je vreme da pozovu FBI. Kao najveći svetski proizvođač softvera za 2D i 3D modeliranje, Autodesk svoje proizvode prodaje arhitektama, dizajnerima, urbanim planerima, modelarima, hipotekarnim brokerima i proizvođačima vozila širom sveta – dakle, čak su i zvanični dobavljač softvera za Grimley Smith, firmu za hemijski inženjering iz Skantorpa.

Ovakav specijalizovani softver nije nimalo jeftin. Pojedinačne licence za Autodeskove profesionalne CAD programe staju od tri do sedam hiljada dolara, što odražava ogromne sume koje se ulažu u istraživanje i razvoj proizvoda.

Godine 2002. Odeljenje za zaštitu od piraterije u toj kompaniji primetilo je da prodavac u Ukrajini nudi nove-novcate verzije jednog Autodeskovog programa za dizajn preko eBaya, za tričavih 200 dolara, dok je cena tog istog proizvoda na malo u redovnoj prodaji iznosila 3500 dolara. „Hmm", pomislili su, „ovde nešto nije u redu!"

Silicijumska dolina pati od istog problema kao i holivudski studiji. Proizvodnja filmova često podrazumeva resurse koji se mogu porediti s onima potrebnim za razvoj složenih softverskih programa. A kako troškovi produkcije rastu, pojava globalne mreže proizvođača falsifikovanih DVD-jeva, neretko povezanih sa sindikatima organizovanog kriminala, umanjila je prihode od filmova. To je naročito vidljivo u recesiji – ako možete da birate hoćete li da pogledate film u bioskopu i platiti 15 dolara za ulaznicu ili ćete ga odgledati na savršenoj DVD kopiji po ceni od samo jednog dolara, potonjem se zaista teško odupreti.

Isto tako, možda upravljate kompanijom u oblasti preduzetništva u kojoj imate pristup, recimo, proizvodu Autodeska. Da biste kupili od njega softver i licence za svoje potrebe, možda morate da se ispružite za skoro 20 hiljada dolara, ali ako ih kupite od tog

Ukrajinca na eBayu, vaš ukupni trošak iznosiće osamsto dolara. Budimo iskreni: možda jeste nezakonito, ali je svakako primamljivo!

Od sedamdesetih godina prošlog veka, kad je softver počeo da postaje komercijalno dostupan, proizvođači uzalud pokušavaju da razviju tehnologiju koja će sprečiti njegovo kopiranje (isto kao u slučaju CD-a i DVD-ja). Nijedna takva tehnologija ne potraje duže od nekoliko dana pre no što je provali neko od desetina hiljada hakera i krakera širom sveta. Za poslednje tri decenije, ispostavila se kao *najdonkihotskiji* ogranak haj-tek industrije.

Istočnoevropski hakeri odigrali su naročito važnu ulogu u krakovanju bezbednosnih podsistema ugrađenih u softver. Osamdesetih, uoči pada komunizma, Sovjetski Savez dao je zadatak raznoraznim saveznicima u svom trgovačkom bloku, zvanom COMECON,[14] da razviju personalni kompjuter i softversku industriju – pre svega u Bugarskoj i Istočnoj Nemačkoj. Osnovne karakteristike komunističkih kompjutera bile su zajedničke celom Istočnom bloku: bili su ružni i neprestano su se kvarili. Izazovi s kojima su se suočavali tvorci novoformirane regionalne kompjuterske industrije bili su tako veliki da su ovi postali neverovatno ingeniozni u prevazilaženju gličeva i bagova.[15]

Zatim, fabrike softvera koje su Istočnoevropljani osamdesetih godina sagradili nisu se devedesetih, posle pada Berlinskog zida, mogle takmičiti sa Silicijumskom dolinom – nije bilo novca za ulaganje u istraživanje ili opremu. Međutim, moćni novi sindikati organizovanog kriminala, koji su imali ogroman uticaj na privredu nekadašnjih komunističkih zemalja, doživljavali su te fabrike kao istinsku šansu. Prvo su se domogli tih postrojenja (mahom na nepošten način), a onda zaposlili one talentovane inženjere da proizvode falsifikovani softver u industrijskim razmerama. Tempo su određivale Bugarska, Ukrajina i Rusija, a ni Rumuni nisu mnogo zaostajali za njima.

Stoga, kad su u Autodesku uočili da jedan prodavac iz Ukrajine na eBayu isporučuje velike količine falsifikovane verzije njihovog proizvoda kupcima u Sjedinjenim Državama, normalno je da su osetili potrebu da preduzmu nešto u vezi s tim. Posle izvesnog većanja pozvali su FBI, koji je pak odmah obavestio

14 Savet za uzajamnu ekonomsku pomoć. (Prim. prev.)

15 Glitch je greška koju napravi kompjuter; bug je softverska greška, „bubica".

državno tužilaštvo u San Hoseu, u Kaliforniji. A pošto je u prevaru bio umešan i eBay, tužilaštvo je smesta pozvalo specijalnog istražitelja Grega Kraba iz Poštanskog inspektorata SAD (USPIS), koji je u to vreme službovao u San Francisku.

Nadležnost u slučajevima sajber kriminala imaju tri kriminalističke službe: FBI (zato što mu je posao da sprečava zločin); Tajna služba (zato što njihov pravilnik obuhvata i zaštitu valute SAD i prevare s kreditnim karticama) i USPIS (zato što ima zadatak da nadzire sve nezakonite aktivnosti povezane s federalnom poštanskom službom). Potonja služba uključila se u sajber igru pre svega zato što prevare koje se izvode putem eBaya i sličnih servisa često podrazumevaju slanje robe poštom (bilo da je nezakonito kupljena ili je deo šeme za pranje novca).

Za proteklih petnaest godina, USPIS je okupio tim za istrage u oblasti haj-tek kriminala, a Greg Krab je bio toliko uspešan da se naposletku preselio iz San Franciska kako bi predvodio Odsek za globalne sajber istrage, iz velike anonimne zgrade u vašingtonskom velikom anonimnom kompleksu zvanom Federalni centar (ne zaboravite da ga precrtate sa spiska znamenitosti koje „morate obići" prilikom posete prestonici SAD).

Krabova tevtonska pojava, pomalo hrapav glas i južnjačko otezanje istovremeno su privlačni i zastrašujući. On je ovlašćeni javni knjigovođa i teško je odagnati osećaj da mu, kad bi vam samo zavirio u finansije, ne bi trebalo dugo da pronađe dokaze o značajnom prekršaju, sve i ako ste čisti kao suza. Ta osobina je Krabu od koristi u njegovom poslu, budući da je, za dobrog sajber policajca, sposobnost da proučava dugačke spiskove brojeva, kratkih poruka i naizgled nerazumljivih podataka *sine qua non*.[16] Samo radno mesto možda zvuči uzbudljivo, ali kao i toliko toga drugog vezanog za informatiku, veći deo posla je iritirajuće dosadan.

Nakon što se upoznao s Autodeskovim slučajem, Krab je ušao prevari u trag tako što je proverio gde su kupci piratizovanih programa slali novac. Ispostavilo se da su uplate vršili na bankovne račune u vlasništvu petnaest „mazgi", građana SAD raštrkanih širom zemlje. Pranje novca i prevare zavise od tih ljudi koji (uglavnom) nisu svesni svoje stvarne uloge, a koji se javljaju na oglase u kojima se nudi dobra zarada za posao koji obavljate na svom kućnom računaru. Od kandidata koji prođu potom se traži

16 Lat.; uslov bez koga se ne može, nešto obavezno. (Prim. prev.)

da dostave poslodavcu broj svog bankovnog računa. U slučaju Autodeska, mazge su dobijale uplate od 200 dolara i potom prosleđivale 180, zadržavajući 20 dolara kao proviziju. Novac su slali banci u Letoniji, jednoj od triju baltičkih država čija je uloga u sajber kriminalu i širem problemu sajber bezbednosti nesrazmerno velika u poređenju s njihovim ukupnim brojem stanovnika, koji iznosi sedam miliona.

Uz pomoć letonske policije, Krab je otkrio da je konačno odredište novca nekoliko bankovnih računa u Ternopolju, na zapadu Ukrajine. Svi računi su pripadali izvesnom Maksimu Kovalčuku ili njegovoj supruzi.

Krabu je bilo jasno da Kovalčuk kao pojedinac neće izazvati kolaps američke privrede. Koliko god je cela rabota ljutila Autodesk, po merilima velikih grupa za organizovani kriminal, Kovalčuk je od ove prevare zarađivao bednu siću. Stoga je Krab poradio na tome da provali u njegov imejl nalog i ustanovi ima li tamo još kakvih tajni, i u izvesnom trenutku stekao „jedinstvenu sposobnost" da prati Kovalčukovu prepisku – što se može protumačiti samo na dva načina: ili je Krab hakovao ciljani kompjuter, ili je ubedio Kovalčukovog imejl provajdera da mu omogući pristup. Kako god bilo, ova „jedinstvena sposobnost" imala je dalekosežne posledice po stvarni svet jer je Krab, skoro čim je počeo da čita imejl prepisku, shvatio da je Kovalčuk umešan u projekt mnogo veći od piratizovanja proizvoda Autodeska: razvoj vebsajta zvanog CarderPlanet.

Iako su Kovalčuk i njegova povezanost s piraterijom ostali primarni fokus njegove istrage, Krab je počeo, gotovo uzgred, da mapira „porodično stablo" CarderPlaneta. Nesvestan da je uveliko na radaru jedne američke kriminalističke službe, Kovalčuk je komunicirao prilično slobodno, i tako je kombinacija sreće i marljivog istraživačkog rada dovela Kraba u zavidan položaj. Ne samo da je inspektor bio u velikoj prednosti što se tiče samog Kovalčuka nego je za dobar korak pretekao i zapadne obaveštajne agencije. Delimično prodrevši u najdinamičniju zajednicu sajber kriminala u svetu, postigao je nešto što obaveštajcima sa Zapada dotada nije pošlo za rukom.

Ipak, iako je Krab uspeo da sazna mnogo o dešavanjima u hakerskoj zajednici Ukrajine, nije mogao da preduzme bogzna šta u vezi s tim. Nije čak mogao ni da uhapsi Kovalčuka. Ne samo da između Sjedinjenih Država i Ukrajine ne postoji sporazum o

ekstradiciji, već su i političke okolnosti koje su vladale u ovoj ogromnoj istočnoevropskoj zemlji bile krajnje nezgodne. Predsednik države bio je Leonid Kučma, koji je predstavljao oličenje razgranate mreže korumpiranih odnosa između oligarha i organizovanog kriminala. Zatim, Sjedinjene Države su se nadmetale s Evropom i Rusijom za uticaj u toj zemlji, a u to vreme je preovladavao prilično siloviti vetar iz pravca Moskve. Pod uslovom da ne napušta Ukrajinu, Kovalčuk je bio bezbedan.

Usred svega toga, inspektora Kraba su potkraj 2002, dok je još bio u San Francisku, pozvali iz bezbednosnog odseka Vise, čije se sedište slučajno takođe nalazi tamo. Njihove ljude izluđivao je ogroman uspeh hakera po imenu Boa, koji je posredstvom svog zloglasnog sajta Boa Factory uspešno ukrao ili pomogao drugima da ukradu desetine hiljada kreditnih kartica. Krab je naćuljio uši – to ime, Boa, znao je iz brojnih razgovora koje je video na Kovalčukovom nalogu. Nije li Kovalčuk mnogo kupovao sa sajta Boa Factory i naučio od njih štosove zanata, i nije li diskutovao o razvoju CarderPlaneta? Poštanski inspektor je vrlo brzo izdvojio Bou i Scripta kao dve ključne figure iza CarderPlaneta. Diskretno, preko Interpola, zamolio je ostale kriminalističke službe da ga obaveste ako uhapse ikakve Ukrajince osumnjičen za haj-tek kriminal.

Krajem februara 2003. Roman Vega vraćao se sa službenog putovanja kući na Maltu, kad ga je neki prijatelj zamolio da usput svrati kod njega u Nikoziju, na Kipru. Vega je to veče proveo pijući s prijateljem i prisećajući se zajedničkih doživljaja u Burmi 1991. gde su bili deo radio-amaterskog tima koji je prvi emitovao signal iz te države pod vojnom vlašću.

Kad se vratio u svoju sobu u hotelu Kasteli, sačekalo ga je neprijatno iznenađenje u obličju Modesta Pojadisa, lokalnog policijskog inspektora, koji je Ukrajinca smesta uhapsio pod optužbom za saučesništvo u prevari s kreditnim karticama, koju je izveo drugi gost iz Ukrajine, a kome je Vega dozvolio da odsedne u njegovoj sobi (loš potez, kako se ispostavilo). Za Vegu, to je bio početak odnosa sa kriminalističkim službama na Kipru i u Sjedinjenim Državama, koji se ne može opisati drugačije nego kao kafkijanski.[17]

17 Vid. Roman Vega: *A Journey: DOSSIER*, http://www.romanvega.com/p/blog-page_30.html. Vegu sad već skoro punih deset godina premeštaju iz jednog američkog zatvora u drugi a da mu još nije suđeno ni za šta od onoga što mu se stavlja na teret. (Prim. prev.)

Pošto je proverio arhiv Interpola, Pojadis je stupio u kontakt sa Gregom Krabom, inspektorom koji je rukovodio istragom o Boi u SAD. Čoveku iz Poštanskog inspektorata SAD rekao je kako veruje da Roman Vega nije niko drugi do glavom Boa. Krab je jedva uspevao da zatomi oduševljenje. Nisu još bili ni završili razgovor, a u mislima je već rezervisao prvi let za Nikoziju. Posredi nisu bili samo izgledi da pokuša da izdejstvuje izručenje jednog od osnivača CarderPlaneta... imali su njegov laptop! Ako su Kiprani uspeli da dokuče njegov alter ego a da ne znaju sa čime tačno imaju posla, zamisli samo šta bi istražitelj kao što je Krab mogao izvući sa tog hard diska.

„Hapšenje Boe predstavljalo je veliki šok", rekao je Xhora, član CarderPlaneta, odražavajući osećanja mnogih svojih sajber zemljaka sa Planete. Boa je bio čovek koji je doprineo da CarderPlanet postane zabavan, a istovremeno zanimljiv i unosan. A pošto je bio znatno stariji i iskusniji od ostalih stanovnika Planete, mnogi su pretpostavljali da mu policija i slični gnjavatori ne mogu ništa.

U isto vreme, Script je, kao rezultat svoje kontrole nad CarderPlanetom, gomilao sve više moći i gotovine. „Njegovi intervjui bili su osmišljeni tako da dodatno popularizuju sajt i pojačaju poslovanje", rekao je Null Name, još jedan predani član CP-ja, „i uspevao je u tome. Sajt je bio preplavljen novim članovima. Ali atmosfera se promenila. Više nije bilo isto."

Prijateljsko druženje iz prvih dana CarderPlaneta zaista je brzo nestajalo. Bez obzira na to, sajt je generisao više novca nego ikada pre. Bila je pokrenuta i sekcija foruma na engleskom jeziku i nije prošlo dugo a na sajt su se učlanjivali karderi iz celog sveta. Međutim, u dalekom San Francisku, Greg Krab je pario oči sadržajem Boinog hard diska, iskopavajući iz njega hiljade tajni koje su razmenjivali Boa i Script. „Uopšte nisam morao da ispitam Bou", rekao je Krab. „Štaviše, ni ne zanima me šta taj tip ima da kaže zato što imam njegov hard disk – ne može mi reći ništa novo!"

U stvari, Krab možda i nije pronašao u kompjuteru baš sve što je želeo. Izgleda da je kriminalistička služba SAD u izvesnom trenutku provalila jedan od enkripcijskih sistema na laptopu marke VAIO, ali da ga je njegov vlasnik bio pojačao moćnim sistemom, Handy Bits EasyCrypto (besplatno se skida s interneta), koji

obezbeđuje da oko 80 odsto kompjuterskih fajlova ostane nedostupno za bilo kakvu pretragu.

Na karderskim forumima je i dan-danas prisutno ogorčenje zato što članovi veruju kako je Roman Vega odrukao Golubova. To nije tačno – svi podaci koje policija poseduje o Golubovu izvučeni su s laptopa VAIO. Ne samo da je Vega ćutao kao zaliven i tako samo naškodio samom sebi, nego je dosad proveo skoro čitavu deceniju u raznoraznim kiparskim i američkim zatvorima, premda još nije osuđen ni za kakav zločin.

Uprkos svim novim informacijama, Krab i dalje nije mogao ništa da preduzme u vezi sa Scriptom. On se nalazio u Ukrajini – za razliku od Maksima Kovalčuka, koji je zajedno sa suprugom uhapšen za piratizovanje Autodeskovog softvera dok je sedeo u mlečnom restoranu u Bangkoku, tri meseca nakon hapšenja Romana Vege u Nikoziji. Baš kao što je Kipar izručio Vegu Kaliforniji, tako je i Kovalčuk s Tajlanda upućen na Zapadnu obalu.

Script nije imao nameru da napušta domovinu i, kako bi se dodatno zaštitio, početkom 2004. objavio je na CarderPlanetu da daje ostavku na položaj i zauvek napušta sajt.

Kao i uvek, Script je imao plan. Karding aktivnosti, koje je nezaboravno opisao kao nešto što radi „mirne savesti", donele su mu dovoljno novca i sada je želeo da ga uloži u zakonite poslove. Možda se nadao da će tako izbeći buduće neprijatnosti. Možda je imao ambicija izvan sajber sfere. Objavio je na CarderPlanetu svoje dramatično saopštenje – predaće upravljanje sajtom svom pouzdanom *konsiljeru* i više se neće pojavljivati na bini Planete.

Čini se da je Script nameravao da okrene list i opere ruke od nepoštenih rabota. Nešto, međutim, ipak nije predvideo.

Revoluciju.

8.
Iznova napisana skripta

Boris Borisovič Popov je telefonirao u kancelariju i rekao da se ne oseća dobro. Objasnio je da mu je lekar savetovao da nekoliko dana odleži. Neke kolege su bile iznenađene. Sitna građa Borisa Borisoviča i njegove mladalačke crte umeli su povremeno da podsete na bolešljivo dete, ali on je verovatno bio najmarljiviji i najdisciplinovaniji među njima. „Bilo je zadovoljstvo raditi s njim", prokomentarisao je kasnije jedan kolega. „U celoj službi nisi mogao naći boljeg čoveka."

Uprkos tome što je uzeo bolovanje, Popov nije legao u postelju, već je – zdrav kao dren – izašao iz svog stana, zaustavio taksi i otišao na kijevski aerodrom Borispolj, gde je čekirao kartu za let do Odese. Kako je poticao iz Donjecka, u istočnoj Ukrajini, i ruski mu je bio maternji jezik, ukoliko bude sačuvao prisebnost, njegovo prisustvo na krajnjem jugu zemlje neće izazvati podozrenje.

Po dolasku u Odesu, seo je u autobus i odvezao se u grad. Bio je vruć julski dan. Temperatura se kretala oko tridesetog podeoka, ali je vedri vetrić sa Crnog mora prijatno osvežavao vazduh. Popov je vrlo brzo našao pogodan stan i iznajmio ga. U roku od nekoliko sati, pristiglo je i troje preostalih članova tima – Nataša Obrizan i gospoda Griško i Baranec. „Nismo smeli da odsednemo u hotelu", objasnio je Boris, „zato što nismo verovali lokalnoj policiji." Samo je jedna osoba u celoj zemlji znala da se oni nalaze u Odesi: bio je to ministar unutrašnjih poslova.

Šest meseci ranije, Ukrajina je doživela dramatičan potres – Narandžastu revoluciju. Toj izuzetno plodnoj zemlji, s potencijalom da snabdeva evropski kontinent manje-više svom hranom koja mu je potrebna, drama nije bila ništa novo. Režimi koji su se u njoj izmenjali u XX veku obuhvatali su ekstremni nacionalizam, autokratiju, komunizam i fašizam, svaki odgovoran za sopstveni brend zastrašujućeg nasilja nad stanovništvom zemlje: građanski rat, masovna glad, genocid, deportacije i opšte siromaštvo.

Najtrajnije domaće zaveštanje ove haotične istorije jeste podela Ukrajine na dva geografska ali i jezička tabora: zapadni i istočni, u kojima se govori ukrajinski odnosno ruski. Prestonica Kijev pruža se između njih kao klimavi most, u nadi da će pomiriti povremeno suprotstavljene tradicije. U najcrnjim vremenima XX veka, zapad zemlje postao je u glavama ljudi povezan sa fašizmom i Nemačkom, dok je istok doživljavan kao grudobran komunizma i Moskve.

Ova podela nije uvek tako jasna – na istoku možete naći oblasti u kojima se govori ukrajinski, dok proruski kandidati neretko zgrnu neočekivano veliki broj glasova u nekim krajevima na zapadu zemlje. Bez obzira na to, korisna je kao empirijsko pravilo. Od sticanja nezavisnosti, Kijev i zapadne provincije teže ka bliskijim vezama s Evropskom unijom i NATO-om, dok istok nastoji da ojača veze s Rusijom. Štaviše, mnogi istočni Ukrajinci još uvek smatraju kako u svakom pogledu pripadaju svom ogromnom susedu.

Do 2004. u Ukrajini su se smenjivale vlade i predsednici koji su podržavali prorusku liniju, umnogome na zadovoljstvo istoka i na nezadovoljstvo ukrajinskih nacionalista na zapadu. Kao posledica toga, odnosi sa EU, NATO-om i SAD bili su vrlo hladni – ukrajinski vladini zvaničnici bivali su ugošćeni u američkim zatvorima, *pod optužbama za pranje novca i ostale Mekmafija aktivnosti*, jednako često kao u Beloj kući.

Međutim, dok su državni činovnici, političari i oligarsi punili džepove na račun običnih građana, čiji se životni standard strmoglavio i pre i posle smene milenijuma, oko dvoje političara „novog stila", Viktora Juščenka i Julije Timošenko, ujedinio se novi politički pokret. Tek kasnije je izbilo na videlo da su i to dvoje „mustre" vrlo slične svojim političkim protivnicima. Juščenko je dospeo na naslovne strane u septembru 2004. nakon što je neko pokušao da ga otruje dioksinom (skoro je sigurno da je to bilo maslo ruskog KGB-a). Preživeo je taj pokušaj atentata, mada znatno unakaženog lica, i objavio da će se kandidovati za predsednika države.

Kampanja za svrgavanje stare garde raspirila je maštu mladih Ukrajinaca, koji su je preobrazili u politički festival nazvan Narandžasta revolucija. Studentski aktivisti iz Srbije,[18] koji su

18 Pripadnici „Otpora" su mesecima boravili u Ukrajini i obučavali mlade za nenasilni otpor u slučaju krađe glasova na izborima zakazanim za 31. oktobar 2004. (Prim. prev.)

pomogli u svrgavanju svog sopstvenog diktatora, Slobodana Miloševića, pristigli su u Kijev kako bi obučavali perspektivne ulične političare svojih gotovo suseda. U zemlju su nahrupili neokonzervativistički prozeliti iz SAD naslutivši realnu šansu da razbiju nos Moskvi i odvuku Ukrajinu bliže orbiti NATO-a.

Taj nagli porast političke aktivnosti bio je od samog početka izložen međunarodnom uplitanju. Kad je Juščenko u januaru 2005. konačno proglašen za predsednika, a Julija Timošenko za predsednicu vlade, Ukrajina je postala vrlo živahno eksperimentalno tle za rusko-američke odnose, koji su se uporno pogoršavali. Oboje novih lidera isticali su ne samo posvećenost Ukrajine ulasku u Evropsku uniju nego i nadu da će zemlja za kratko vreme postati članica NATO-a. Premda je ovo bilo osuđeno na propast (najzad, dobilo je podršku svega 30 odsto ukrajinskih glasača), Moskva je njihov postupak protumačila maltene kao objavu rata.

Za četiri godine koliko je prošlo otkako je prvi put natrapao na Maksima Kovalčuka, čoveka koji je prodavao piratske kopije Autodeskovog softvera, inspektor Greg Krab je strpljivo razvijao odnose s kolegama iz zbunjujućeg niza raznoraznih službi u sklopu ukrajinske policije. Međutim, iako je stekao važne kontakte, učtivo su odbijali sve njegove zahteve za hapšenje Dimitrija Golubova, poznatog kao Script.

Sve su to promenili dramatični događaji iz decembra 2004. i januara 2005. kad su na vlast došli Juščenko i Julija Timošenko. Krab je shvatio da Narandžasta revolucija predstavlja priliku koju ne sme propustiti. Ubrzo posle burnih događaja pozvali su ga iz Ambasade SAD u Kijevu. Saznao je da je ukrajinsko Ministarstvo unutrašnjih poslova već očišćeno od tvrdokornih starih konzervativaca i da je postavljen novi tim, skloniji saradnji sa Zapadom. „Odmah dolazi ovamo!", rekli su mu. Čoveku iz Poštanskog inspektorata nije trebalo dvaput reći.

U Kijev je stigao u junu 2005. i podneo zvaničnicima Ministarstva unutrašnjih poslova dokaze u vezi sa slučajem Golubov. Dve nedelje kasnije, inspektor Popov, iz Odseka za borbu protiv organizovanog kriminala, našao se na putu za Odesu, s instrukcijama da uđe u trag neuhvatljivom Scriptu i uhapsi ga.

Popov je znao da zadatak nije nimalo lak. Više od svega pribojavao se da informacija o tome ne procuri, jer ako vesti o raciji stignu u Odesu pre njega, čitava operacija će propasti pre no

što i počne. Kao uspešni karder koji je u toj fazi konačno dosegao status višestrukog „dolarskog milionera", Golubov je sebi izvesno kupio zaštitu lokalne policije. Na svom terenu bio je nepobediv.

Dovženkova ulica leži oko tri kilometra južno od najužeg centra Odese. Ulice su tu oivičene drvećem i taj kraj se ubraja među otmenije adrese u gradu. Golubov je živeo u stanu svoje babe; kad su se Popov i njegov tim popeli, s iznenađenjem su ustanovili da im pristup brane teška čelična vrata. Nakon što su zauzeli položaje, Popov je dao kolegama znak. „Otvaraj! Policija!", povikali su i zalupali na nepomična vrata. Dočekala ih je tišina i napregnuto su osluškivali ne bi li čuli bar nešto iza čelične barijere – jednom od njih se učinilo da je čuo tihe korake, ali uprkos svim njihovim naporima, vrata su ostala čvrsto zatvorena.

Dok se Popov pitao da li da pozove u pomoć neku tešku mašineriju, osetili su u nozdrvama jedak miris gorućeg papira. „Bože!", pomislio je, „počeo je da uništava dokaze!" Ne časeći ni časa, Popov je obavestio jedinicu za hitne intervencije i ubrzo su stigla vatrogasna kola. Dok se vrelina povećavala, vatrogasci su probili rupu u zidu stana i kroz nju počeli da zasipaju unutrašnjost penom. Kad je izgledalo da će industrijske hemikalije sasvim poplaviti bakin stan, Golubov je konačno zaključio da je igri došao kraj i otvorio je vrata.

Prizor je bio bizaran. Ne samo da je Popov zatekao Golubovljevu arhivu u plamenu nego je haker istovremeno ubacivao kompjuterske diskove u Raskat. Da je Golubov prosto obrisao fajlove iz svojih kompjutera, to ne bi predstavljalo bogzna kako velik izazov ni za koga s osnovnim poznavanjem kompjuterske forenzike ko bi pokušao da ih rekonstruiše. Papir možete da spalite – s kompjuterskim fajlovima to mnogo teže ide. Međutim, elektromagnetni pulsni generator ruske proizvodnje, poznat kao Raskat, emituje snažne elektromagnetne talase kojima u potpunosti uništava podatke. Golubov je bio uhvaćen na delu i Popov ga je sproveo u Kijev, gde je zatvoren.

Sada su se i Vega i Golubov nalazili pod ključem (isto kao i više ostalih ključnih članova porodice CarderPlaneta). Obojica su neumorno poricali da su oni zapravo Boa i Script. Još nijedan nije osuđen – štaviše, prvi je proveo sedam godina u američkim zatvorima a da protiv njega nije započet pravi sudski proces, što za

sobom povlači ozbiljna pitanja o efikasnosti američkog krivično-pravnog sistema.

Bez obzira na tačan uzrok, CarderPlanet je ostao bez svog jezgra. Vizionarski sajt za hakere i krakere je možda nestao, ali njegova zaostavština je neizmerno velika – CarderPlanet je radikalno promenio kriminalitet na Mreži.

Uz to, krupni sajber kriminal je već bio prerastao svoje ukrajinske korene. Administratori CarderPlaneta su poslednje dve godine podsticali razvoj foruma na engleskom jeziku, koji je postojao uporedo sa ruskim diskusionim grupama. Taj forum širio je duh Odese među hakerima i karderima u celom svetu. Dva njegova člana bila su početnici, ali duboko zaintrigirani novim svetom profesionalnog kardinga. Jedan je za svoj avatar uzeo veselog pirata, a drugi sliku iz omiljenog filma mnogih gikova: na scenu stupaju JiLsi i Matrix001.

Deo III

9.
Tigar, tigar

Kolombo, Sri Lanka, 1988.

Tras! Tras! Tras!

„Otvaraj! Otvaraj!"

Vojnici u takvom raspoloženju retko kad sačekaju odgovor; pogotovo ne u pola šest ujutru. Puškama su razbili vrata i navrli u kuću. Pretražujući prostoriju po prostoriju, naredili su članovima porodice da poležu na pod, a onda sve ispreturali.

Kad su galama i svetlo ispunili kuću, troje dece se užasnuto trglo iz sna. „Ustaj! Ustaj!" Deca su se preznojavala mada su bila samo u donjem vešu, ali vrlo brzo su počela da cvokoću od straha. Vojnici su izdvojili najstarije, dečaka od samo jedanaest godina, i uprli prstom u beli deo kože, veličine dlana, na njegovom stomaku. „Šta je ovo? Šta je ovo?", uzviknuli su gotovo pobedonosno. „On koristi eksplozive!"

„To je beleg koji imam od rođenja", odvratio je on. „Samo beleg, ništa više."

Odvukli su dečaka u stranu i poseli ga na stolicu u dnevnoj sobi, a onda počeli da ga saslušavaju. Roditelji i baka preklinjali su vojnika koji im je izgledao kao glavni u grupi i konačno se i on složio kako je malo verovatno da žgoljavi dečkić, koji još ni u pubertet nije ušao, pravi bombe za Tamilske tigrove.

Mali Renu je bio navikao na takve gungule jer drugo nije ni pamtio. Pet godina ranije, u julu 1983, kao šestogodišnjak bio je evakuisan iz Kolomba. Tamilski gerilci ubili su trinaest pripadnika vojske Sri Lanke. Rulja Sinhaleza izmasakrirala je stotine nedužnih Tamila u glavnom gradu Kolombu,[19] čime je započet

19 Sinhalezi ili Singali su narod koji čini 75 odsto stanovništva Šri Lanke. Tamili čine nešto manje od jedne četvrtine, ali, globalno gledano, višestruko su brojniji od Sinhaleza. (Prim. prev.)

dugotrajan građanski rat, koji se završio tek dvadeset šest godina kasnije.

Ostati u Kolombu dok razularene grupe Sinhaleza divljaju po gradu nije više bilo moguće, stoga su se Renuovi roditelji spakovali i odveli svoje troje dece u Džafnu, centar tamilske zajednice u Sri Lanki. Taj grad nalazi se na samom severnom špicu zemlje i samo ga osamdeset kilometara deli od jugoistočne obale Indije. U to vreme bio je i glavno uporište tamilske gerile. Otpor vladi u Kolombu, u kojoj su glavnu reč vodili Sinhalezi, stalno je rastao.

Nije prošlo dugo od Renuove selidbe, a nepredvidljivo nasilje građanskog rata i stalnih pobuna počelo je da se prikrada sve bliže njegovom novom domu. Godine 1987. vladine snage držale su Džafnu pod opsadom u nastojanju da se izbore s raznoraznim naoružanim grupama, a naročito s ozloglašenim Tamilskim tigrovima (Oslobodilački tigrovi tamilskog Elama – Liberation Tigers of Tamil Eelam, LTTE). Broj izbeglica koje su preko Palkovog moreuza bežale iz grada u južnu Indiju dosegao je kritičnu masu, što je ubedilo vladu u Nju Delhiju da mora da dela. Po dogovoru postignutom sa srilankanskom vladom, Indijci su u Džafnu poslali velike mirovne snage da nadziru sprovođenje mirovnog sporazuma.

Nije prošlo dugo, a odnosi između indijskih mirovnjaka i Tamilskih tigrova su se pokvarili i Džafna je ponovo postala jedan od najopasnijih gradova na kugli zemaljskoj. U oktobru 1987. indijske trupe bile su odgovorne za masakr nad nekoliko desetina nedužnih civila u glavnoj gradskoj bolnici. Bio je to jedini incident u četvrt veka dugom građanskom ratu koji je naveo vladu u Kolombu i Tigrove da se ujedine u svom revoltu. Za Renua i njegovu porodicu bilo je previše opasno da ostanu u Džafni, pa su se uputili natrag na jug, u Kolombo.

Jednog popodneva, Renuov otac je poslao dečaka da kupi neke namirnice. Renu još nikad nije video toliko rupija i gurnuo ih je u džep zajedno sa spiskom onoga što je trebalo da kupi. Na putu do prodavnice spazio je pored puta čoveka koji je igrao nekakvu igru. Tu su bila tri lončeta, a ispod jednog nalazio se kamenčić. Renu je posmatrao kako se ljudi klade jedni protiv drugih na ovo ili ono lonče nakon što im vešti zabavljač brzinom svetlosti izmenja mesta. Bio je opčinjen i nikako mu nije bilo jasno kako to igrači nikako ne uspevaju da pogode gde je kamenčić, dok je on sam svaki put pogodio. Progurao se u prvi red i izvukao zgužvane očeve novčanice. Jedna po jedna nestajale su u

čovekovom džepu dok je Renu, baš kao i oni pre njega, bezuspešno pokušavao da pokaže pravo lonče. Međutim, što je više gubio, to se grozničavije kladio. Nesvestan koliko je izgubio, naprosto nije bio u stanju da se zaustavi – sve dok nije ostao bez novčanica, a njegovo malo telo, ošamućeno od adrenalina, naglo se oblilo ledenim znojem pri pomisli na očevu tešku ruku podignutu iznad njegove glave. Nikad se više nije kockao.

U godinama koje su prošle od odlaska iz Džafne, situacija u prestonici se donekle smirila mada bezbednost njenih tamilskih stanovnika nikad nije bila sasvim zagarantovana, što je jasno pokazao i upad vojske u njihovu kuću. Renuovoj porodici je, međutim, ponestajalo mogućnosti.

Renu, koji još nije bio zašao u tinejdžerske godine, veći deo života proveo je bežeći od zla u gore i natrag, ponekad doslovno izbegavajući unakrsnu vatru. Ubrzo posle upada vojske u njihovu kuću, kad je nedorasli dečak zbog urođenog belega zamalo bio proglašen teroristom, Renuova baka je zaključila da je za njega, kao Tamila, sazrevanje u glavnom gradu Sri Lanke previše pogibeljno. Mogao bi se naći u iskušenju da se priključi Tigrovima ili pasti kao plen nacionalističkih singaleških grupa koje su krstarile gradom.

Do 1992. porodica je nekako skrpila dovoljno novca da pošalje Renua u London, gde su mu živeli tetka i teča.

Taj novi život na drugom kraju sveta, u krajnje nepoznatom i nimalo bliskom okruženju, sadržavao je neke druge opasnosti. Sitan i mršav kao grana, Renu se u gimnaziji Lengdon – jednoj od najvećih i najnepokornijih u istočnom Londonu – našao u procepu između dveju velikih zajednica, belačke i bengalske. Matematika mu je išla odlično, bio je najbolji u razredu, ali je jedva uspevao da se izražava na engleskom. Kao potpunog autsajdera, nemilosrdno su ga maltretirali i, posle šest meseci, jednostavno je odbio da više odlazi u školu, uprkos preklinjanjima očajnih tetke i teče.

Renu je dve godine proveo takoreći zatvoren u kući; dešavalo se da nedeljama ne izađe na vazduh. Sva njegova aktivnost svodila se na gledanje televizije od jutra do večeri.

Renukant Subramanijam je naučio kako da bude sam.

I možda bi sam i ostao da ga teča nije naposletku primorao da se vrati u spoljni svet, konkretno, u srednju stručnu školu Njuham. Tamo je naučio štošta što dotad nije znao: kako da se druži

s vršnjacima; kako da puši marihuanu; kako da ispija „martelov" konjak; i kako da programira kompjuter.

U lokalnom pabu, naduvan i pijan, Renu je pobedivao virtualne protivnike u arkadnoj igrici *Street Fighter*. Koliko je mladih bilo opsesivno privučeno tom hipnotički repetitivnom izazovu, koji je bacao njihov avatar u borbu na život i smrt protiv niza podjednako agresivnih boraca? Je li to krotilo agresiju ili ju je podjarivalo? Je li protok dopamina oko čeonog moždanog režnja, koji iniciraju ove igrice, doveo do izrazite zavisnosti kod svih mladih ljudi ili samo nekih od njih?

Renu je neumorno stajao za mašinom, natapajući organizam adrenalinom a mozak endorfinima. Kad bi završio, još sav napet i u grču, sljuštio bi „martel" da se povrati i smiri. Ta dvostruka navika polako je počela da predstavlja namet na njegov oskudni džeparac. *Street Fighter* mu je postao važniji no ikad. Kad bi legao da spava, u mislima su mu se u tehnikoloru pojavljivali nasilni prizori iz igrice.

Kao što je nekad prestao da se kocka, tako je sad odlučio da prestane da igra i da nikad više ne pipne arkadnu mašinu. Nažalost, njegova tadašnja odluka odnosila se samo na igricu *Street Fighter*, a ne na njegovu rastuću sklonost piću i drogama.

To što je prekinuo s igranjem igrice nije značilo i kraj njegove opčinjenosti kompjuterima uopšte. Zavoleo ih je još kad se prvi put poigrao njime, kao devetogodišnjak u Sri Lanki. Zbog oskudice novca nikad nije imao redovan pristup kompjuterima, ali je u svojim ranim dvadesetima prevazišao taj problem tako što je prihvatio da studira informatiku na londonskom Vestminsterskom univerzitetu.

Ubrzo potom Renu je otkrio *warez*, piratizovani softver čiji su bezbednosni sistemi krakovani i koji se potom distribuirao među entuzijastima kolektivno poznatim kao Scena (The Scene).

Bio je to svet u kojem je mogao biti s prijateljima i sâm, sve u isto vreme.

10.
Teorija igre

Ajslingen, Baden-Virtemberg, 2001.

Baš u vreme kad je Renu tek počeo da istražuje Scenu, 800 kilometara odatle, u južnoj Nemačkoj, još jedan mladi korisnik kompjutera slučajno je naleteo na istu tajanstvenu zajednicu.

Petnaestogodišnji Matrix001 se zaljubio. Ne u devojku. Matrixu su glavu zavrtele kompjuterske igrice. U prvo vreme bile su samo jedan aspekt u uravnoteženoj i normalnoj adolescenciji, i nadmetale su se za udeo u njegovom slobodnom vremenu sa gimnastikom i školskim orkestrom u kom je svirao klarinet. Posmatrano spolja, nije bilo ničega neobičnog u vezi s njim. Lako je skrivao svoju tajnu opsednutost igricama. Niko nije znao – ni njegovi drugovi, ni roditelji, ni braća i sestre – osim, možda, njegovog mlađeg brata.

Ne samo da je obožavao igrice već ih je i veoma vešto igrao i, dok se kraj školske godine približavao, njegovo sedenje za tastaturom počelo je da se proteže do kasno u noć. Ispostavljalo se, međutim, da je držanje koraka s najnovijim igricama skup sport, pogotovo ako ti je (kao u Matrixovoj ekipi) renome rastao kad objaviš da si uspešno savladao neku tek objavljenu igricu.

Do 2000. godine tržište je bilo preplavljeno novim igricama sa bleštavom grafikom. Serijal *Pokemon* izbacivan je brzo i u velikim tiražima, dok su se, od onih nešto ekstremnijih, kao veliki hit ispostavili *WWF Smackdown 2: Know Your Role*, kao i *Grand Theft Auto*, čiji su zapleti imali nasilni i pornografski pečat. Matrix se sve vreme očajnički trudio da se domogne najnovije igrice, ali naprosto ih nije mogao sebi sve priuštiti.

Što se tiče strasti prema igricama, njegov život je ličio na Renuov. Sem toga, nisu imali ničega zajedničkog.

Rešen da zadovolji strast koja je upravljala njime, Matrix je otkrio internet zajednicu poznatu kao Scena fXp. Ovaj fenomen bio je važan trenutak, ne samo u Matrixovom životu nego i u parametrima internet kulture koji su doživljavali naglu promenu.

Tokom dve decenije, koliko je prošlo od pojave personalnih kompjutera, među njihovim tvorcima, prorocima i najposvećenijim korisnicima razvila se uzavrela – mada nimalo javna rasprava – o njihovoj upotrebi i ulozi u društvu. Većina kriminalnih veština na Mreži proizašla je iz suštinske podele u filozofskoj raspravi koju je generisao internet.

Jednostavno rečeno, rasprava se s jedne strane vodi između onih koji smatraju da je najvažnija njegova komercijalna uloga i, s druge strane, onih koji tvrde da je on pre svega društvena i intelektualna alatka čija sama priroda menja fundamentalni moralni kodeks masovnih komunikacija. Za prve, svako kopiranje kompjuterskog „koda" (stenogram za kompjuterski jezik kojim je napisan softver ili program) koje nije izričito odobreno predstavlja prestup. Potonji su, međutim, ubeđeni da postupak puštanja softvera u promet podrazumeva i odricanje od autorskih prava.

Suština tog pitanja otkrivena je još davne 1976. kad se Bil Gejts otvorenim pismom obratio „hobistima", labavoj grupi koja je obrazovala začetak onoga što će evoluirati u gikove, hakere i krakere. Gejts je u tom pismu izrazio žaljenje nad činjenicom da 90 odsto korisnika Microsoftovog prvog programskog jezika, Altair BASIC, nije došlo do njega tako što ga je kupilo. Umesto toga su ga kopirali, što je značilo da Gejts nije ostvarivao profit na ogromnu količinu rada i novca uloženog u njegov razvoj. Iako je Gejtsov jezik bio slika i prilika neugladenosti zajedničke mnogim gikovima, poruka je bila jasna: optužio je hobiste za krađu.

Hobisti, gikovi, hakeri – „krakeri", kako su kasnije postali poznati – nisu se slagali s njim. Što se njih ticalo, čim je „kod" izbačen na tržište, počinjao je lov na njega. Na Zapadnoj obali, ali i na Masačusetskom tehnološkom institutu (Massachusetts Institute of Technology, MIT) u Kembridžu, u Masačusetsu, neki od najvažnijih svetskih graditelja kompjutera i prvih korisnika bili su zaraženi jakom dozom „kumbaja" ideologije, prema kojoj bi ova tehnologija trebalo da zbliži ceo svet i, iz nekog (nepoznatog) razloga, ne podleže autorskim pravima koja tradicionalno važe u književnosti, muzici i ostalim vidovima stvaralaštva.

Jasno je *zašto* se tako nešto moglo dogoditi: javnost u prošlosti nije bila u položaju da odštampa nelegalni primerak knjige ili proizvodi piratizovane otiske longplej ploča, budući da nije imala potrebnu mašineriju. A sve i da jeste, ta mašinerija je bila glomazna i nepokretna, a policija bi joj lako ušla u trag u nastojanju da zaštiti intelektualnu svojinu.

Kod ili softver je nešto drugo. Posle prelaska s kasetnih uređaja, na kojima su se početkom osamdesetih godina prošlog veka pisale prve kompjuterske igrice namenjene kućnoj upotrebi, proizvodio se na flopi diskovima, CD-ovima, DVD-jevima i hard diskovima koji su postajali sve manji i zgodniji za korišćenje. Otprilike u to vreme, Konglomerat proizvođača komercijalnog softvera (Empire of Commercial Software Producers) prvi put je pokušao da uzvrati udarac, tako što su u svoje proizvode počeli da ubacuju dodatni kod, namenjen da spreči neovlašćeno kopiranje njihovog materijala. CD-ovi i kasete su rutinski imali digitalnu zaštitu.

Premda je kao taktika sasvim razumljivo, proizvođačima se ovo obilo o glavu. Davne 1982. još jedan nemački tinejdžer, koji je kasnije postao poznat pod zagonetnim hakerskim nadimkom MiCe!, konačno je ubedio roditelje – mada su oni i dalje verovali da greše – da mu za Božić kupe kompjuter. Ali nakon što su dali toliki novac, odbili su da mu daju ijedan jedini novčić za igrice, ne shvatajući da je, što se njihovog sina tiče, kompjuter potpuno beskoristan bez softvera za igrice, koji se u to vreme pisao na kasetama.

Shvatio je da jedini način da koristi kompjuter jeste da pozajmljuje softver od drugova i kopira ga. Jednom prilikom je ustanovio da ne može da prekopira sadržaj kasete. Probao je na sve moguće načine, ali je kompjuter svaki put kraširao. Danima i noćima se izluđivao, a onda je konačno na jednom mestu na traci uočio nekakav kod, koji naizgled nije imao nikakvu funkciju. Potom mu je sinulo: taj kod blokira proces! Kad je to shvatio, MiCe! je mogao da počne da eksperimentiše ispisujući kod različitim redosledom sve dok ga jedne noći – bingo! – nije provalio.

Prvi gejmeri, kao što je bio MiCe!, bili su inspirisani da provaljuju digitalnu zaštitu zato što su bili zavisni od igrica, a ne zato što su hteli da zarade. Kopije su se prenosile od jednog do drugog gejmera i tako se rodila Scena.

To je još uvek bio naporan i dugotrajan proces, budući da je obuhvatao fizičko kopiranje koda na novu kasetu. Bez obzira na to, gejmeri su revnosno reagovali na rukavicu koju su im bacili proizvođači igrica i uskoro je procvetala supkultura krakera. Jedini cilj njenih pripadnika bio je da krakuju igrice i ostali softver onog časa kad se pojave na tržištu i da se potom razmeću pred ostalim krakerima svojom veštinom.

Tako je rođeno sajber podzemlje, mada će vrlo brzo početi da se deli na vrlo različite zajednice – neke dobre, neke loše.

11.
Nema povratka

Skoro dve decenije nakon što je MiCe! krakovao svoju prvu kasetu, mladi Matrix našao se suočen s istom dilemom. Bio je navučen na igrice, ali nije mogao da ih priušti. Dilema je bila ista, ali je tehnologija u međuvremenu napredovala gotovo do neprepoznavanja. Igrice su se sada dičile sofisticiranom grafikom koja je oduzimala dah, zamršenim zapletima i neverovatnim izazovima.

Opsesija mnogih gejmera pojačala se u skladu s tim. Kasete i flopi diskovi su već bili muzejske vrednosti, a vreme je isticalo i CD-romovima, DVD-jevima i memorijskim karticama (pre no što su i izumljene). Igrice su sve više bile kadre da postoje samo kao kod na internetu. Međutim, ne možete uskladištiti mnogo njih na svom kućnom PC-ju. Štaviše, to su bila vremena dial-up modema, kad je kačenje na internet podrazumevalo višesatno zauzeće telefonske linije. Ali ako ste sa svog kućnog kompjutera mogli da pristupite mnogo većem kompjuteru, tada ste mogli da skladištite i šerujete onoliko igrica koliko želite...

fXp je skraćenica za File Exchange Protocol, ali sve što treba da znate o fXp-ju jeste da omogućava veoma brz prenos podataka između dvaju kompjutera. Naročito je koristan za razmenu podataka među serverima. Važno je naglasiti da je server prosto kompjuter prilagođen da funkcioniše kao komunikacioni hab.[20] Tako će neka velika kompanija, na primer, imati vlastiti server koji svim zaposlenima omogućava pristup internetu. Mnogi serveri su veliki i jaki, i njihov pristup Mreži ne zavisi od telefonskih linija.

fXp internet forumi ujedinili su bratstvo čiji su pripadnici upadali na servere i potom ih koristili za skladištenje i igranje igrica. Matrix je brzo učio i nije prošlo dugo a njegov kompjuter je prečešljavao internet u potrazi za serverima.

---

20 Eng. *hub*, mrežni uređaj koji spaja komunikacione linije u jednoj centralnoj lokaciji. (Prim. prev.)

Koristeći automatski program, njegov kompjuter je na Mrežu slao bezbroj poruka koje su, u suštini, kucale na vrata servera koji su mogli biti locirani bilo gde u svetu. Kad server otvori vrata, Matrixov kompjuter bi upitao: „Smem li da uđem?" Većina servera bi mu na to odgovorila: „Koja je lozinka?" Međutim, pronašao je sasvim dovoljno servera čiji se administratori nisu potrudili da stave lozinku, u kom slučaju je Matrixova mašina dobijala odgovor: „Naravno, samo napred. Tvoj sam i radi sa mnom šta god hoćeš, zločesti glavni kompjuteru!"

Matrix je administratore koji ostavljaju svoje kompjutere tako nezaštićenim smatrao nedostojnim čak i prezrenja. Mogao je da uđe ko god hoće i ukrade tajne kompanije. Kao kad bih ja, razmišljao je, otišao u tržni centar s prepunim novčanikom, a onda ostavio novčanik nasred tržnog centra i otišao.

Zatim, bilo je i servera čije je lozinke bilo lako pogoditi, kao što su oni kod kojih je bila postavljena fabrička lozinka, obično nešto poput „admin" ili – najgluplja moguća lozinka na svetu – „lozinka".

Kod nekih drugih kompjutera nalazio je pak slabe tačke u njihovom bezbednosnom sistemu (možda slabo korišćen „port" ili tačku ulaska na kojoj se nije tražila lozinka), koje je mogao eksploatisati za dobijanje pristupa unutrašnjem mehanizmu servera. Većini korisnika kompjutera to je možda ličilo na atomsku fiziku, ali za Matrixa to nije bilo ništa komplikovanije od pritiskanja kvake na otključanim vratima i mogao je za pola sata naučiti bilo koga kako se to radi.

Prvi zadatak koga je Matrix morao da se lati, nakon što preuzme kontrolu nad serverom, bio je da popravi one iste slabe tačke koje je upotrebio da bi ušao: morao je da osigura da ga niko drugi ne može napasti onako kako je on to uradio.

Ušavši na server, bio je u položaju da ga kontroliše. Mogao je, ako želi, da motri svu dolaznu i odlaznu elektronsku poštu i internet saobraćaj. Međutim, nije to želeo: hteo je samo da koristi te servere za primanje, skladištenje i distribuiranje igrica uz pomoć fXp tehnologije.

Matrix je imao samo petnaest godina, ali bio je u stanju da po volji zalazi u ogromne delove interneta za koje većina odraslih i ne zna da postoje. Njegovi roditelji nisu imali pojma o tajnom svetu koji je istraživao iz svoje sobe. Niti je postojala verovatnoća da će saznati – daunloudovanje igrica i softvera bilo je,

razume se, nezakonito i predstavljalo je kršenje zakona o autorskim pravima, ali praksa je u to vreme bila ograničena na vrlo mali broj korisnika. Proizvođači su je smatrali smetnjom ali ne i nerešivim problemom. Ogromna većina igrica kupovala se savršeno legalno u prodavnicama ili na sajtovima poput Amazona.

Matrix svoju aktivnost od roditelja nije skrivao zbog zabrinutosti da možda krši zakone o intelektualnoj svojini. Ne – shvatio je da je za tinejdžere, u vezi s internetom, najlepše to što tvoji roditelji nemaju (i u većini slučajeva nikad i ne mogu imati) ni najbledu predstavu šta radiš. Njima je bilo sasvim dovoljno teško da prate koji DVD-jevi ulaze u kuću ili izlaze iz nje. Međutim, DVD-jevi su barem bili fizički predmeti koje su majka ili otac mogli da konfiskuju ako saznaju da njihov trinaestogodišnjak gleda filmove za odrasle (svaki put se, dabome, izlažući opasnosti da izazovu zamornu provalu besa).

Internet je sve to menjao. Deca su odrastala u sajber okruženju koje je njima bilo jasno samo po sebi i sasvim normalno, ali je za roditelje bilo sve tajanstvenije i sve teže za snalaženje. Tinejdžeri su bili savršeno svesni da su im roditelji na tom sajber moru potpuno izgubljeni, što je počelo da pojačava osećaj da je Mreža oblast njihovog mladog života iz koje se roditelji mogu legitimno proterati. Koliko je majki i očeva ušlo u sobu i videlo svoje tinejdžere kako uz kratak blesak rumenila na obrazima uvlače svoj internet pretraživač u dno ekrana? A ako makar samo okrznu pogledom stranicu na Fejsbuku, čak i ako joj klinci pristupaju na javnom mestu, dete se smesta preobražava u borca za ljudska prava, optužujući mučenog roditelja da se ponaša kao gestapovac.

Ono čega su mnoga deca i tinejdžeri manje svesni jeste da, premda roditelje uspevaju da prevedu žedne preko vode, postoje najrazličitiji ljudi koje nije tako lako prevariti – i kojih ima sve više. Među njima mogu biti patološki progonitelji, oglašivači, siledžije, pedofili, policajci, nastavnici i kriminalci. Samo najsofisticiraniji korisnici umeju da zataškaju ono što zaista rade na Mreži.

Nasuprot strpljivim napaćenim roditeljima, te druge zainteresovane strane su, uz malo kompjuterske pismenosti, počele da prate digitalne stope koje su deca i tinejdžeri vremenom počinjali da ostavljaju. Takve zabeleške mahom obuhvataju priznanja o uzimanju droge i nalivanju alkoholom, vređanje nastavnika,

maltretiranje školskih drugova i, sve više, postovanje sopstvenih pornografskih portreta. Možda roditelji ne znaju za to, ali drugi ljudi znaju. Čak i istinski pametni klinci kao što je Matrix umeju da postanu previše sigurni u sebe.

Time što je zaposedao loše zaštićene servere i igrao igrice preko njih, Matrix zapravo nije radio ništa loše. Na prelazu milenijuma, u Nemačkoj to nije bilo protivzakonito, a pitanje autorskog prava je u digitalnoj eri bilo nejasno – tinejdžeri i mladi su već počeli da šeruju muzičke fajlove koristeći Audiogalaxy i Napster. Bili su to vebsajtovi na kojima te, ako hoćeš da daunloudueš „Bohemian Rhapsody" grupe Queen, na primer, upute na PC negde u svetu na kom je ta pesma pohranjena. Potom, koristeći vebsajt kao most, možeš da učitaš kopiju tog muzičkog fajla na svoj kompjuter.

Za veoma kratko vreme, milioni ljudi su shvatili da više ne moraju da kupuju snimljenu muziku – sve je bilo dostupno besplatno! Dok je fajl-šering za proizvođače kompjuterskih igrica bio samo manja smetnja, muzičkoj industriji predstavljao je ogroman problem. Da bi se izborili s njim, biće im potrebni pravnici koji će redefinisati autorsko pravo za digitalnu eru; zatim će morati da nateraju zakonodavce da donesu zakone u tom duhu; naposletku, moraće da ubede policajce da im je hapšenje digitalnih pirata u opisu radnog mesta. Štaviše, muzička industrija moraće da razvije nove tehničke uređaje kako bi sprečila tu praksu (u čemu je dosad slavno propala).

Praksa šerovanja muzičkih fajlova, malih i lako prenosivih s jednog kompjutera na drugi, raširila se kao šumski požar. Prodaja nosača zvuka u SAD dosegla je vrhunac 1999. sa zaradom od nešto više od 14,5 milijardi dolara, ali je naredne godine počela da opada, a taj trend traje i danas.

Nasuprot tome, neovlašćeno daunloudovanje igrica, koje su mnogo veće i kao takve nezgrapne za rukovanje, jedva je i ostavilo traga na prodaju fizičkih CD-ova i DVD-ijeva, koja iz godine u godinu raste. Štaviše, oni koji daunlouduju igrice pomažu u njihovom reklamiranju. Prema tome, najgore što se može reći o Matrixovoj sajber aktivnost jeste da mu je krala san i terala ga da zapostavlja učenje.

Međutim, tada je Matrix, a da gotovo ni sam nije primetio, sišao mali korak niže niz spiralu nesmotrenosti.

Reklamna industrija je otkrila internet i, kao i svi ostali, pokušavala da smisli kako će ga najbolje iskoristiti. Mreža je oglašivačima ponudila izrazite prednosti – kao prvo, mogao si preciznije ciljati potencijalnu publiku. Ako hoćeš da prodaješ pelene, tada izbegavaj vebsajtove posvećene skajdajvingu i koncentriši se na forume za mlade roditelje. Ukoliko plaćaš oglašavanje na televiziji, radiju ili bilbordima, skajdajveri ti se neminovno mešaju u ciljnu grupu, od čega nemaš nikakve vajde (sem, naravno, ako skajdajveri slučajno nisu i mladi roditelji).

Kao drugo, možeš da uskladiš uspešnost i troškove oglašavanja. Svaki put kad novopečeni mama ili tata kliknu na oglas za pelene, to registruju i proizvođač pelena i oglašivač. Firma za reklamiranje tada je plaćena po broju klikova. Oglašivači i prodavci potom mogu da analiziraju takozvanu „stopu klikova" (Click Through Rate, CTR), tako da naš proizvođač pelena može videti da, od stotinu posetilaca sajta namenjenog skajdajverima, niko nije kliknuo na oglas. Međutim, na forumu za mlade roditelje, na oglas je kliknulo deset od njih sto, što daje CTR od 10 procenata – a firma za reklamiranje biće plaćena u skladu s tim. Nije prošlo dugo, a CTR je iznedrio „isklikavanje" (click fraud).

U jednu takvu šemu bio je umešan administrator jednog od foruma koje je Matrix posećivao. Podstakao je Matrixa da servere koje je kontrolisao upotrebi za postavljanje programa koji će, u određenim intervalima, automatski kliknuti na banere s oglasima. Matrix je za svaki klik dobijao po cent. Nije ni znao da je posredi nezakonita rabota. Potom mu je administrator rekao da postoji još jedan forum na kom se raspravlja o sličnim stvarima i da bi trebalo da ga pogleda. Upravo na tom forumu, CarderPlanetu, Matrix je prvi put čuo za prevaru s kreditnim karticama.

Rubikon je prešao u psihološkom transu, uopšte ne videći vode što su se oko njega talasale. Bio je dete i klizio je u kriminal, polagano, malo po malo. Negde u pozadini uma je možda i znao da nešto nije u redu, ali granice su u sajber prostoru veoma zamagljene – ako se uopšte i vide.

12.
Put u Indiju

Čenaj, Tamil Nadu, 2001.

Dve hiljade prve navršilo se devet godina kako Renu nije video roditelje, braću i sestre. Ipak, čak i mladi ljudi poput njega, koji su silom prilika naučili da preživljavaju bez bliskih veza s porodicom, povremeno imaju obavezu da popuste pred majčinim preklinjanjem. Posle mnogo nagovaranja, obećao joj je da će nabaviti pare da doleti u Tamil Nadu, na jugu Indije, i poseti porodicu.

Do para je, međutim, teško dolazio. Dok je studirao na Vestminsterskom univerzitetu, Renu je našao posao u Pizza hutu, kao radnik na isporuci. Radio je do ponoći ili jedan ujutru, a onda morao da ustane rano kako bi prisustvovao prvom predavanju (premda je njegova tačnost, kako je godina odmicala, sve više opadala). Taj posao mu je prvi put u životu doneo malo dodatnog novca. Međutim, nije ga bilo toliko da bi mogao da uštedi: sve što mu je ostajalo odnosila mu je zavisnost od droge, koja je sada obuhvatala kokain, ali Renu će vrlo brzo prihvatiti i onaj najstrašniji narkotik, krek kokain.

Kako nije uspeo da sakupi pare za kartu, Renu ih je pozajmio od prijatelja i, pre dugog leta za Čenaj, za svaku sigurnost, kupio putničke čekove American Expressa u vrednosti od 3.000 funti.

Niko nije znao šta da očekuje od susreta: bio je još dečak kad je otišao od majke. Sad je bio mladi čovek čiji je život bio obeležen razdobljima velike usamljenosti. Društveni život mu se posle koledža poboljšao, ali nije bio sklon neobaveznom ćaskanju niti nekom velikom ispoljavanju osećanja. Mada mlad, brzo je gomilao mrlje na svojoj prošlosti. Postojalo je mnogo toga što neće pričati svojima.

Putovanje nije dobro počelo. Iz Čenaja, morao je da se odveze na selo jednim od onih pretrpanih, zagušljivih indijskih autobusa, deleći prostor sa previše ljudi, previše živine i previše prtljaga. Negde na polovini puta, kad su mu se oči same od sebe sklopile posle dugog leta iz Londona, osetio je lagani trzaj koji ga je načas probudio. Pomislio je da mu se učinilo. Međutim, kad se iskrcao iz autobusa, radost zbog ponovnog susreta s majkom bila je pomućena – torbica mu je bila prosečena, a putnički čekovi vredni 3.000 funti nestali.

Ali najgore je tek imalo da dođe. Kad je otišao u filijalu Ameksa u Čenaju, odbili su da mu nadoknade štetu (u čemu se, kako je njemu bilo objašnjeno, i sastoji cela poenta nošenja čekova umesto gotovine). Pre no što mu izdaju nove čekove, morao je da od lokalne policije donese potvrdu da mu je novac ukraden. Takođe su mu rekli da Ameks ne garantuje povraćaj novca, već da će odluku o tome doneti „nakon što razmotre slučaj".

Kad se vratio u Englesku, birokrate u Ameksu bile su isto tako bezosećajne. Uporno su tvrdili kako Renu nije dostavio neophodnu dokumentaciju koja bi dokazivala da su čekovi ukradeni ili izgubljeni. Od naknade štete nema ništa.

Ljudi od kojih je pozajmio novac bili su mu prijatelji. Međutim, samo do izvesne granice. Saosećali su s Renuovom mukom, ali su ipak hteli svoj novac natrag. Renu je pak gotovinu mogao da namakne samo ako izvadi kreditne kartice – uostalom, ovo je Doba plastike, a banke i kreditne kompanije su priželjkivale Renua za klijenta kao i svakoga drugog.

Bedni posao u Pizza hutu nije mogao da pokrije njegove narastajuće finansijske potrebe: dugove, piće i drogu, troškove studija, stanarinu. Tlo pod Renuovim nogama pretilo je da se izmakne. Obaveze na fakultetu su prve počele da trpe. Nakon što je, stanujući u kampusu Harou pri Vestiminsterskom univerzitetu, dao ispite iz prve godine, počeo je da sve češće propušta predavanja. Nije položio ispite iz druge godine, niti mu je to uspelo u drugom roku.

Da bi zaboravio na beznađe, počeo je mahnito da daunlouduje pesme s Napstera, da bi potom otkrio sajt na kom su pripadnici Scene razmenjivali igrice i krakovane programe. Dok je Renu tonuo u bezbedan i dalek svet na treperavom ekranu, daleko od hijena stvarnosti koje su kružile oko njega, njegove noći postajale su sve duže.

Jedne večeri, ispričao je nekom od brojnih lutajućih surfera koje je susretao na netu i svom IRC kanalu o novcu koji Ameks odbija da mu isplati. „Idi na *amexsux.com*", rekao je njegov kontakt. „Ako ništa drugo, makar ćeš se osećati malo bolje!"

Renuu se mnogo dopao taj sajt (logo: *DO leave home without it*),[21] na kom su bivši klijenti American Expressa izražavali svoj gnev zbog postupaka koje su doživeli kao nepravdu. Animozitet javnosti prema ovoj kompaniji je poveliki, o čemu svedoči i Google pretraga: postoje stotine sajtova posvećenih pljuvanju po Ameksu, a na mnogima se može naći impresivna zbirka linkova koji vode do negativnih medijskih izveštaja o kompaniji.

Jedan od članova foruma nudio je originalnu zamisao onima koji su imali pritužbi na ovu kompaniju. „Osvetite se! Idite na *CarderPlanet.com*!"

Davši se u potragu za CarderPlanetom, Renu je smatrao da je došlo vreme da se pozdravi s vlastitom ličnošću. Postao je JiLsi, čiji je avatar bio crtani lik nestašnog pirata s crvenim šeširom i crnim povezom preko levog oka. Pravi kapetan Džek Sperou na sajber Karipskom moru, kad je najzad bacio sidro na CarderPlanetu, u gruboj ekipi hakera, krakera i prevaranata vrlo brzo se osetio kao kod kuće. Negde u toj grupi osobenjaka lutao je Matrix i premda je prošlo nekoliko meseci pre no što su razmenili zavete o virtualnom prijateljstvu, njih dvojica su postali poznati na mnoštvu sajtova koji su težili da imitiraju CarderPlanet.

Gde biste drugde mogli naći zavisnika od droge izbeglog sa Sri Lanke kako se druži s uobraženim nemačkim tinejdžerom iz srednje klase, a sve pod okriljem harizmatičnog Odešanina s vizijom nove Ukrajine? Samo na Mreži.

21 Eng.: *Izlazite iz kuće bez njih* – parafraza poruke koju zaštitna lica kompanije American Express još od 1975. ponavljaju u reklami za putničke čekove, a koja glasi: „Don't Leave Home Without It" tj. „Ne izlazite iz kuće bez njih."

13.
Shadowlands

Njujork, 2003/04.

RedBrigade je zaključio da je kucnuo čas da udari na Vašingtonski uzajamni fond (Washington Mutual Bank) – u njegovim očima, ta ustanova nije bila ni manje ni više do snabdevač besplatnim novcem. Banka je, zapravo, 1983. izgubila status uzajamnog fonda, i sada je njen generalni direktor obznanio da namerava da ova poštovanja dostojna ustanova sa sedištem u Sijetlu postane „Volmart bankarstva". Zavrni slavinu gde god je to moguće, glasila je šefova filozofija. Prebacuj zajmove i ne zagledaj previše imovinu i kreditnu sposobnost klijenata. Odobri kredit za refinansiranje onima koji ne mogu da otplaćuju hipoteku. Ulaži što je moguće manje u osoblje i opremu. To je bilo jeftino bankarstvo, lišeno svih ukrasa. Srećom po RedBrigadea i njegove pajtaše, ti ukrasi su obuhvatali i elementarne bezbednosne sisteme.

Iz hotela Four Seasons u Pedeset sedmoj ulici br. 57 izašao je oko 11 pre podne. Još je bio mamuran od sinoćnje žurke, ali kako je šampanjac bio iz dobre berbe, a kokain skoro potpuno čist, osećao se više nego ornim za akciju.

Stigavši do banke, ležerno je prišao činovnici koja nije prošla obuku („njih nisu morali mnogo da plaćaju") i pružio joj WaMu debitnu karticu.

„Koliko danas želite da podignete, gospodine?"

„Deset hiljada, molim vas."

„Nema problema!"

Tap-tap, tap-tap. Ovde u WaMu, RedBrigade je morao da preda karticu činovnici, koja ju je potom provukla kroz uređaj na

blagajni. U svakoj drugoj banci, to je trenutak kada bi se činovnici na monitoru mogla pojaviti šifrovana poruka da se „odmah javi". RedBrigade bi morao pažljivo da proučava njeno lice. Da li me upravo provaljuje? Treba li da zbrišem? Ili da naprosto stojim ovde kô kreten i čekam da se pojave panduri? A možda je sve u najboljem redu i samo sam paranoičan?

Ne i u WaMu. Te cicije nisu htele da se isprse za kompjuterske monitore i šifrovane bezbednosne poruke. Stoga bi RedBrigade, ukoliko se desi da u ovoj ustanovi odbiju njegovu karticu, prosto delovao malčice iznenađeno, a onda bi se izvinio i otišao. U WaMu niko nije pozivao policiju.

Međutim, njegove kartice nikad nisu bile odbijene. Tog decembarskog dana 2003. žena je provukla njegovu karticu, a uređaj ju je bez problema prihvatio. RedBrigade je potpisao odštampanu priznanicu na kojoj se nalazio kod transakcije, a potom prišao bankomatu u prednjem delu banke. Ukucao je kod. Nekoliko trenutaka čekanja i onda je mašina, poput ćudljivog „jednorukog bandita" u kasinu u Las Vegasu, počela da bljuje keš u pedesetica-ma: 1.000, 2.000, 3.000... sve dok RedBrigade nije strpao u džep dvesta novih novčanica od pedeset dolara.

Ponekad se činilo kao da su banke namerno ostavile svoje bankomate otvorene za njega i njegove prijatelje. Tako je lako, pomislio je, kao da smo odabrani za ovo. Naročito je uživao da izvlači novac iz Citibanka. Ako je ijedna banka to zaslužila, to je bio Citi. Pre svega, najnemoralniji su od svih tih bankarskih skotova. A drugo, imaju bedno obezbeđenje.

Phishing (fišing) tj. „pecanje" je od samog početka bilo ključno za sve vidove sajber kriminala. Čak i ako kompanija ima dobro zaptivenu digitalnu odbranu, relativno neiskusan haker može da je probije fišing napadom. Reč je o slanju ogromnog broja mejlova na adrese koje se ponekad ciljaju zbog toga što pripadaju određenoj kompaniji – banci, na primer – a ponekad su nasumično odabrane. Mnoge spam poruke sadrže zaraženi prilog (attachment) ili link koji, ako se na njega klikne, usmerava pretraživač na sajt koji može automatski učitati malver. Ako haker pošalje nekoliko miliona spam imejlova, ne treba mu veliki procenat odgovora da bi mu se trud isplatio – svaki ugroženi kompjuter obećava pristup bankovnim računima i ostalim ličnim ili finansijskim podacima.

Banke se oduvek suočavaju s gadnom bezbednosnom glavoboljom: svojim klijentima (mada to nije izgovor za zastrašujuće slabe sisteme obezbeđenja u prvih petnaest godina internet bankarstva). Čak i najbolje umreženi sistemi dobri su samo onoliko koliko i njihov najslabiji element – a mi, stotine miliona njihovih klijenata, ranjivi smo u najvećoj mogućoj meri.

Prema tome, ako ne može da upadne u banku, sajber lopov obratiće se za pomoć njenim klijentima. Poslaće vlasnicima računa milione imejlova koji izgledaju kao da su poslati iz njihove banke, i potom sačekati odgovore: brojevi računa i lozinke sručuju se kao lavina.

Bilo je prosto kô pasulj odraditi fišing klijenata Sitibanka:

Kupi gomilu tek hakovanih mejl adresa. ✓
Kupi Dark Mailer, vlažni san spamera. ✓
Kupi proksije. ✓
Kupi hosting. ✓
Dizajniraj novu veb stranicu Sitibanka. ✓
Ubaci pop-up prozor koji neće da se skloni dok se ne unesu broj kartice i PIN. ✓
Odvoji mejl adresu na koju će se slivati brojevi računa i lozinke. ✓

RedBrigade je svakog dana odlazio na pecanje. Proučavao je podatke na računu izvesne dr H. M. Hebert iz severnog dela države Njujork. „Hmmm... živi blizu. Jebote, zarađuje pedeset soma mesečno, a njen jebeni muž inkasira više od sedamdeset dva soma!" Zagledavši malo pažljivije, video je da meta radi na Volstritu. Da je doneo bolje odluke u životu, razmišljao je, mogao je da krade legalno, kao taj tip... Međutim, nije smeo da dozvoli sebi da se zanosi takvim maštanjima – umesto toga, prosto je počeo da računa. Dakle: dva tekuća računa, dva štedna računa, jedan dozvoljeni minus i jedna kreditna kartica... po 2.000 dolara sa svakog. Ukupno: 12.000 dolara od jedne ribe.

A na njegov račun je svakog dana doplivavalo pedeset takvih ribica.

Terevenka u njujorškoj filijali Vašingtonskog uzajamnog fonda trajala je tek malo više od dve nedelje, donevši mu skoro 300.000 dolara. Što je bilo baš dobro, budući da su se njegovi prosečni nedeljni troškovi kretali negde oko 70.000 dolara. Svaka

dva do tri meseca kupio bi novi besni mercedes ili BMW. Putovanje prvom klasom se podrazumevalo. O kupovini novog ručnog sata marke Breitling razmišljao je isto kao kad neko od nas kupuje novine. Posedovao je prelep apartman na Aper Vest Sajdu, ali tamo je provodio samo dve ili tri noći nedeljno, zato što je uživao u boravku u luksuznim hotelima u gradu. RedBrigade je zarađivao više od fudbalera Premijer lige u Engleskoj, ali bez poreske stope od 50 odsto.

Ništa mu nije bilo nedostižno. Izvlačio bi pedesetice iz svežnja gotovine i video onaj izraz na licu blagajnika, koji je značio: „Jebote, ko je ovaj lik?" Verovao je da sigurno misle da je bogati mladi lezilebović ili diler droge. Međutim, u Dobu plastike superbogati nose farmerke i majice jednako često kao odela najčuvenijih krojača iz Savil Roua. U svakom slučaju, trgovci su uvek uzimali novac – juveliri, dileri automobila, vlasnici vinoteka, hotelijeri – niko nije postavljao nikakva pitanja. Otkud su znali: možda taj neobrijani tip poseduje Google? I, uostalom, koga je briga kako je zaradio pare?

Nešto ga je stalno kopkalo. Imao je previše gotovine. Jedne večeri je došao kući sa 77.000 dolara u džepu, na onih 300.000 koliko je već imao u stanu. Tu su bile i naplative novčane uputnice u vrednosti 110.000 dolara. RedBrigade je bio pokrenuo globalnu operaciju isplate, kako bi dostavljao podatke s kartica i računa istočnoevropskom posredniku, koji je organizovao pohare bankomata i potom mu slao gotovinu. Zbog te operacije, RedBrigade je ponovo morao da se lično poduhvati posla s bankama. Smučilo mu se više da se trudi da ostane u okviru sume koja nije podlegala proveri – naime, propisi namenjeni sprečavanju pranja novca nalagali su da se svaka transakcija preko 10.000 dolara mora registrovati u Ministarstvu finansija. Sranje, pomislio je, ko bi ga znao da je ovako teško rešiti se novca!

Pripremao je još jednu isplatu od 77.000 dolara. To će biti obična šetnja, svega nekoliko blokova od njegovog stana, a onda je pomislio: „Imam ovde toliko novca, stvarno ne mogu da se gnjavim time." Bilo mu je jasno da s celom tom slikom nešto žestoko nije u redu. Međutim, kroz glavu mu je prolazilo samo: „CarderPlanet je bio jedno, ali ko bi ikad poverovao u ovo Shadowcrew ludilo? Ko bi poverovao da mogu da uđem u banku, svakog božjeg dana, i izađem sa pedeset soma u džepu? Pa to je van svake pameti!"

Kad je CarderPlanet 2004. konačno zatvoren, dičio se ne samo forumima na ruskom i engleskom jeziku nego i dodatnim sekcijama na korejskom, kineskom, pa čak i arapskom. „CarderPlanet je promenio pravila igre", rekao je E. Dž. Hilbert, bivši specijalni istražitelj FBI-ja, koji je proveo nekoliko godina u istrazi ovog sajta. „Svi koji su potom usledili uzimali su CarderPlanet kao svoj uzor. Ne preterujem kad kažem da je on raširio praksu hakerskog kriminala na sve četiri strane sveta."

Sajtovi napravljeni po uzoru na CarderPlanet nicali su na sve strane: *theftservices.com, darknet.com, thegrifters.com* i *scandinaviancarding.com*. Bilo ih je još mnogo, uključujući i jedan s divnom skraćenicom, parodijom na američke akademske zajednice, IAACA (International Association for the Advancement of Criminal Activity, Međunarodno udruženje za unapređenje kriminalne aktivnosti).

Međutim, nijedan nije bio tako uspešan kao Shadowcrew za dve godine postojanja. A RedBrigade je bio samo jedan od mnogih kardera na Shadowcrewu koji je ubo premiju. Kriminalističke službe su tek počinjale da bivaju svesne razmera ove rabote. Banke nisu znale šta da rade, a običan svet nije imao pojma ni o čemu.

Hakeri su bili daleko ispred njih i posvuda je vladao Mamon – menadžeri hedž-fondova, oligarsi, arabijski naftaši, latinoamerički moguli mobilne telefonije, nova crna ekonomska elita u Južnoj Africi, stara bela ekonomska elita u Južnoj Africi, kineski proizvođači globalnih tričarija, tehno-gurui od Bangalora do Silicijumske doline.

Stotine kardera zgrnule su ogromno bogatstvo za vreme postojanja Shadowcrewa; mnogi su bili dovoljno naivni da sve spiskaju na šljašteću propratnu opremu novokomponovanih bogataša. U to vreme, kupovina preko interneta nije obuhvatala proveru IP adrese vašeg kompjutera. Na kreditnim karticama nije postojao sistem verifikacije adrese (Address Verification System): robu ste mogli otpremati u ceo svet (osim u Rusiju i ostale bivše sovjetske republike), bez obzira na to gde je kartica izdata, i niko je ni u jednoj fazi nije proveravao.

Ovaj novi vid kriminala uhvatio je koren i daleko izvan svog rasadnika u ruskoj i ukrajinskoj govornoj oblasti, i počeo da se spontano globalizuje. RedBrigade se prisećao kako su iskusni azijski kriminalci sada komunicirali sa studentarijom iz Masačusetsa koja je razgovarala s Istočnim Evropljanima, čiji su kompjuteri bili

prepuni „dampova" kreditnih kartica. Iza nekih nadimaka na sajtu Shadowcrew krili su se zločinački aglomerati poput Svevidećeg fantoma (All Seeing Phantom), veoma poštovanog među kolegama.

Dobrih deset godina stariji od većine članova sajta Shadowcrew, RedBrigade nije smatrao da bi imao ikakve koristi od priznanja i poštovanja stečenih usponom u hijerarhiji. Nikako mu nije bilo jasno zašto obični članovi gaje takvo strahopoštovanje prema moderatorima i administratorima foruma. Uprkos uspehu sajta, ponašanje menadžera Shadowcrewa imalo je nekakav detinjasti, skoro deranski aspekt – što nije bilo iznenađujuće, s obzirom na to da je većina bila u kasnim tinejdžerskim ili ranim dvadesetim godinama. Uočio je da su CarderPlanet pokrenuli i razvijali pravi kriminalci, dok su mnogi iz Shadowcrew tima bili diletanti čiju su beskrajnu uobraženost nezamislive sume novca koje su zarađivali samo podjarivale.

Što se dalje RedBrigade držao od tih likova, verovatnoća da će ga policija primetiti bila je manja. Svi sem vrlo malobrojne grupe članova Shadowcrewa bili su potpuno nesvesni da je Tajna služba prodrla veoma duboko u sajt.

U aprilu 2003. uhapšen je mladi Amerikanac kubanskog porekla Albert Gonzales, jedan od najviših starešina sajta. Među karderima je bio poznat kao CumbaJohnny. Međutim, nisu znali da je posle hapšenja postao doušnik, čime je Tajna služba ostvarila kritično važan napredak. Gonzales je vodio takozvanu Virtualnu privatnu mrežu (Virtual Private Network, VPN), putem koje su međusobno komunicirali glavni glumci sajta. Pravilno održavan VPN u velikoj meri otežava, ako ne i sasvim onemogućava detekciju od strane kriminalističkih službi – osim, dabome, ako onaj ko pomaže administratorima ne pomaže i policiji, kao što je radio Gonzales.

Dvadeset šestog oktobra 2004. Tajna služba SAD pokrenula je seriju racija širom Sjedinjenih Država, koja je dovela do hapšenja i podizanja optužnice protiv devetnaest osoba zbog njihove uloge u *shadowcrew.com*. Kasnije ih je uhapšeno još nekoliko.

„Shadowcrew je", glasila je optužnica za zločinačku zaveru, „bila međunarodna organizacija sa približno četiri hiljade članova, koja je podsticala i omogućavala široki spektar kriminalnih aktivnosti." To je bilo pravo slavlje za mladu ekipu sajber policajaca, pripadnika Tajne službe. Optužnica izneta pred okružnim sudom u Nju Džersiju zvučala je dramatično. „Administratori su",

glasila je dalje, „kolektivno kontrolisali smer organizacije, donoseći svakodnevne odluke i baveći se dugoročnim strateškim planiranjem zarad kontinuiranog opstanka i razvoja... Administratori su imali neometan pristup kompjuterskim serverima zaduženim za hosting sajta Shadowcrew i, u skladu s tim, bili su u celosti odgovorni za fizičko upravljanje, održavanje i bezbednost tih servera, kao i za sadržaj sajta."

Obaranje Shadowcrewa dočekano je s velikim oduševljenjem u medijima, koji su otišli toliko daleko da su nagoveštavali kako je posredi virtualni ekvivalent uništenju klana Korleone na Siciliji. Naročita halabuka digla se i zato što je među optuženima bila i jedna žena, Karin Anderson, poznata kao Kafka, mada je Tajna služba zapravo propustila da obelodani da je stvarni kriminalac bio njen dečko, koji je prosto koristio njen kompjuter i IP adresu za sopstvene kriminalne radnje. Teško da je to iznenađenje, s obzirom na činjenicu da je 96 procenata hakera muškog pola.

Hapšenja su nesumnjivo bila opravdana. Međutim, jesu li „administratori" bili oni koji su zarađivali od Shadowcrewa? Ne, nisu. Tačno je da je među njima bilo nekoliko takozvanih „monetizera" tj. onih koji su se bavili unovčavanjem (među kojima je glavni bio Gonzales, koji je, bez obzira na svoje bliske veze sa Tajnom službom, kasnije orkestrirao još poznatiju provalu – hakerski upad u bazu podataka kreditnih kartica T.J.Maxxa).[22]

Policija se, međutim, našla suočena s problemom koji će često iskrsavati: hakeri nisu tipični kriminalci. Tačno, stvarni kriminalci eksploatišu njihove veštine za počinjavanje stvarnih zločina protiv stvarnih ljudi. Ali hakeri su neretko nesvesni tog aspekta svoje aktivnosti. Oni su Scriptovi „vukovi samotnjaci", često nezainteresovani za bogaćenje, i više teže da se uzdignu kao majstori među sebi ravnima. „Morate da razumete", objašnjavao je JiLsi osvrćući se na svoje kardersko iskustvo, „da je sve to bila samo igra. Kao kad igraš Grand Theft Auto, samo što to radiš u stvarnosti. Suprotstavljaš se pandurima od krvi i mesa. A osećaj je mnogo lepši! Radi se o poštovanju. Radi se o..." Nakratko je zastao, zbog efekta: *„O tvom ugledu."*

U jednom pogledu, međutim, hapšenje Shadowcrew kriminalaca koji su operisali na internetu repliciralo je efekat koje je

22 T.J.Maxx je američki lanac robnih kuća u vlasništvu kompanije TJX. Gonzales je za ovo osuđen na dvadeset godina robije. (Prim. prev.)

imalo obaranje mafijaške organizacije u stvarnom svetu. Stvorilo je vakuum u kardingu i iniciralo monumentalnu borbu za prevlast među narednom generacijom kardera, okupljenih oko dva nova sajta koja su se naredne godine pojavila: CardersMarket i Dark-Market.

Deo IV

14.
I dođe Iceman

Santa Klara, Kalifornija, oktobar 1998.

Maks Vižn bio je iznenađen kad su se na njegovim vratima u Santa Klari pojavili Kris i Majk, njegova dva kontakta iz filijale FBI-ja u San Francisku. Trećeg čoveka nije poznavao, mada je docnije saznao da je to bio šef FBI-jevog odseka za kompjuterski kriminal. Ali opet, to nije bila obična poseta. „Skupljamo dokaze protiv tebe, Makse", rekli su. „Ovog puta si žestoko uprskao stvar."

U stanju blagog šoka, Vižn je predao svoj kompjuter i sve ostalo – nije hteo da izgleda kao da ometa pravdu, a u isto vreme nije bio ni sasvim siguran u čemu je problem.

Živeo je dobro – odlično, štaviše. Pošto je ostavio za sobom burnu mladost, preselio se iz Ajove u krajeve u kojima gikove, neurednu dugu kosu i konjski rep nisu smatrali neobičnim ili neuglađenim. Niti je ikome bilo čudno to što je svoje prozaično prezime Batler promenio u Vižn. Brzo se navikao na lagodni način života na Zapadnoj obali i, povrh svega toga, bio je veoma zaljubljen u Kimi, svoju buduću suprugu.

Sa svojih dvadeset i nešto, Maks Vižn bio je genije za kompjutersko obezbeđenje i jedan od najuglednijih i izuzetno cenjenih konsultanata u Zalivskoj oblasti. Takođe, bio je i građanski orijentisan momak koji je pokrenuo sajt *whitehats.com*, posvećen pomaganju ljudima i kompanijama da se osiguraju protiv zlonamernih sajber napada. Gospodin Vižn je u svojim postovima ukazivao na najnovije „rupe" u popularnom softveru i objašnjavao kako ih je moguće zakrpiti.

Rupe su bile sve što je hakerima trebalo jer su predstavljale jedan od glavnih pravaca do kompjutera trećeg lica. Reč je o

digitalnim rupama u oklopu softverskih i kompjuterskih sistema, koje su promakle proizvođaču. Kada primeti da je haker, iskoristivši neku konkretnu slabu tačku, provalio u Windows ili neku univerzalnu aplikaciju poput PDF čitača, kompanija poput Microsofta ili Adobea mogla je da je koriguje ili „zakrpi" („patch") tako što će napisati specifičan bezbednosni fiks („fix"), kako se to popularno naziva. Potom je obaveštavala svoje klijente da daunlouduju i instaliraju taj fiks, čime se preprečavao put do klijentovog kompjutera. Ako korisnik ne ažurira softverski lek, kompjuter je još uvek mogao da postane žrtva virusa koji su koristili tu slabu tačku.

Superhakeri koji se bave ispitivanjem sigurnosti kompjuterskih sistema, poput Vižna, često uoče slabe tačke pre svih ostalih i zato je on, kao svaki dobri komšija, davao korisnicima praktične savete kako da se zaštite.

Međutim, njegova dobra dela išla su i dalje od toga. Pružao je besplatne usluge filijali FBI-ja u San Francisku, a federalci su drage volje prihvatali njegovu pomoć.

Za Maksa Vižna nijedan izazov na Mreži nije bio preveliki, nijedna slaba tačka previše sitna da je primeti. Da bi ih pronašao, međutim, morao je, naravno, neprestano da čačka kompjuterske sisteme. Bio je svestan da ga to stavlja u samo središte velike nedoumice, koja je imala prilične posledice po kompjutersku industriju. Kako biste se zaštitili od zlonamernih, tzv. „black hat" ili „crnih" hakera, ponekad je neophodno da etički – „white hat" ili „beli" – haker utvrdi kako je sve moguće provaliti u sisteme, čin koji može biti nezakonit sam po sebi.

Skoro je neizbežno da „beli" hakeri njuškaju po velikim javnim kompjuterskim sistemima, baš kao i „crni". Razlika je u tome što prvi neće koristiti slabe tačke koje nađu za ličnu dobit, dok potonji najverovatnije hoće.

Radeći u maloj kući koju je delio sa Kimi, Vižn je ustanovio da nije u stanju da se odupre porivu da koriguje svaku anomaliju ili problem na koji naiđe na kompjuterskoj mreži. Godine 1998. otkrio je opasnu slabu tačku na mrežama koje opslužuju više vladinih službi, među kojima su bili i delovi Pentagona. Posredi je bila rupa u odbrani, kroz koju su mogli da se provuku svi mogući zlonamerni crvi. Vešti hakeri s bilo koje tačke u svetu mogli su da ugroze doslovno stotine hiljada vladinih kompjutera. Ponovo demonstrirajući svoj patriotizam, Vižn je, kako bi osigurao

bezbednost države, popunio te rupe digitalnim cementom: više nikad niko neće moći da iskoristi tu slabu tačku sistema u pojedinim ministarstvima.

A onda je došlo do prekretnice.

Delovalo je beznačajno, tada kao i sad. Bilo je sićušno, postupak toliko brz da ga je i vreme jedva zabeležilo: elektronski impuls koji je gotovo nemoguće konceptualizovati; jedan dodir tastera; jedno slovo na mnoštvu stranica kompjuterskog koda, najobičniji uslovljeni refleks rođenog hakera. Naime, Maks Vižn je u svim tim vladinim kompjuterima ostavio otvorenu jednu jedinu malu, malecku rupu kroz koju je mogao da se provuče samo on; posle izvesnog vremena, sokolovo oko sajber istražitelja iz Vazduhoplovnih snaga SAD spazilo je tu rupu i pronašlo put do njenog tvorca.

Zato su, dakle, njegovi prijatelji iz FBI-ja zakucali na vrata njegove kuće u Santa Klari i obavestili ga da su nad njim počeli da se nadvijaju crni oblaci. „Izazvao si silne probleme, Makse", rekli su mu. „Ovo je sad pitanje nacionalne bezbednosti – zato se Vazduhoplovstvo uključilo u celu stvar."

Vižn je bio zbunjen i ozlojeđen. Već je ranije, naime, poslao imejl nadležnima i rekao im za svoje sumnje u pogledu ranjivosti sistema i kako planira da ih skenira kako bi ih testirao.

Koliko je ozbiljan bio njegov zločin? Njegovi postupci nisu bili motivisani finansijskom ili nekom drugom dobiti. Naprotiv, činio je veliku uslugu tim federalnim službama. Između ostalog, Vižn je obezbedio kompjuterske sisteme u vojnim bazama i postrojenjima za nuklearna istraživanja, među kojima su bili i nacionalne laboratorije u Brukhejvenu i Livermoru. A s obzirom na to da je šteta koju je izazvao bila minimalna i da ništa nije ukrao, je li pametno podići optužnicu za takav prestup protiv jednog od najtalentovanijih kompjuterista Amerike?

Vazduhoplovčevo otkriće nije dovelo samo do hapšenja Maksa Vižna pod optužbom za puštanje kompjuterskog crva u internet saobraćaj. Posledice su bile još gore: ona malecka rupa ubušena u ulazne portove kompjuterskih mreža rasla je i rasla sve dok se nije pretvorila u strašni ambis, Kazneno-popravnu ustanovu Taft (Taft Correctional Institution), federalni zatvor smešten u pustinji severno od Los Anđelesa. Vižn je odlazio u zatvor kao zreli, iskusni haker, a ne kao kriminalac. Profesionalne kriminalce je upoznao samo u ćaskanjima sa svojim kontaktima iz FBI-ja.

To je imalo da se promeni, naravno, kad je Maks (sa svojim hakerskim umećem) završio u zatvoru s niskim obezbeđenjem, čiji su mnogi kažnjenici robijali zbog prevare i drugih finansijskih zločina.

Maksova situacija nije izgledala nimalo dobro. Međutim, postala je još gora. Ne samo da je poslat u Taft na izdržavanje dvogodišnje kazne nego je, mesec dana pošto je stigao tamo, Kimi izjavila da ga napušta.

Nakon što ga je žena ostavila zbog drugog muškarca, a dotadašnji prijatelji iz FBI-ja odbacili, Maks Vižn se strmoglavio u provaliju na čijem je dnu ležala duboka depresija. Prizemljio se pored kolege zatvorenika, izvesnog Džefrija Normingtona, koji mu je pružio ruku prijateljstva onda kada to niko drugi nije hteo.

Po izlasku iz zatvora, Vižn nije uspevao da nađe redovan posao plaćen više od minimalca. Konkurisao je u kompanijama u inostranstvu i dobijao ponude za rukovodeća radna mesta, ali pošto je bio na uslovnoj kazni, nije mogao da dobije pasoš. U Silicijumskoj dolini pak niko nije hteo da zaposli nekog čija je biografija obuhvatala i neizbrisivu mrlju u vidu osude za kompjuterski kriminal.

Njegovi dugovi postajali su sve veći, a očajanje sve dublje. A onda se jednog dana pojavio njegov prijatelj Normington obećavajući izlaz iz provalije i povratak pod sunce Kalifornije. Put je bio posut sve samim poslasticama. Normington mu je obećavao vrhunski laptop marke Alienware, obavezan ali skup komad hakerskog pribora. Pri tom je to bilo samo za početak. Rekao je će naći Vižnu stan i plaćati mu stanarinu. Sve će Normington da sredi.

U zamenu za neke usluge.

Kriminal nije bio jedina Vižnova opcija. Postojale su i druge mogućnosti koje je mogao da ispita. Mogao se obratiti porodici i prijateljima. Međutim, bio je umoran, osećao se napušteno, a Normington je bio ubedljiv. Još jedna prekretnica; još jedno pogrešno skretanje.

Maks Vižn, pozitivac u svakom pogledu, odbačen je natrag u provaliju. Umesto njega pojavio se Iceman[23] – negativac u svakom pogledu, mada onaj čiji je alter ego, Vižn, nekada sarađivao sa federalcima.

23 Eng., sleng: plaćeni ubica; kradljivac nakita; hladnokrvna osoba. (Prim. prev.)

15.
Cardersmarket

Iceman je sa strane gledao kako je Tajna služba SAD nadmudrila mozgove koji su stajali iza Shadowcrewa. Smatrao je kako nema ničega zajedničkog s tom jeftinom ekipom čiji je cilj bilo džeparenje bezazlenih pojedinaca na netu, dok je istovremeno dozvoljavala da je potkazivači, cinkaroši i deratori izjedaju iznutra.

Sad kad je Shadowcrew odsvirao svoje, a veliki broj karderskih sajtova u pokušaju iznikao da ga zameni, Iceman je rešio da pokaže svetu kako možeš da pobediš zakon. Iznad svega, hteo je da pokaže svoju nadmoć nad sajberspejsom i njegovim korisnicima.

Za Icemana, karderski sajtovi bili su divlja tržišta na kojima je novac bio jedva važan, a sloboda delovanja je značila sve. Iskreno je verovao da se stvaranje specijalnih tržišta, kao što je bio njegov sopstveni novi sajt, CardersMarket, na kojima ljudi mogu razmenjivati informacije, samo po sebi ne bi trebalo smatrati prestupom, čak i ako možda nadahne nekog od trgovaca na nezakonite radnje. Njegov i slični sajtovi bili su signal da Mreža, za razliku od ostalih oblasti života, ne bi smela da oseća kako je sputava teška ruka države, a na naslovnoj strani se vrlo direktno obratio policiji i administratorima na internetu:

PORUKA ZA KRIMINALISTIČKE SLUŽBE, HOSTING & ISPS:

> CardersMarket je *legalni* forum osnovan kao mesto gde je članovima dozvoljeno da diskutuju o temama po svom izboru. Nije dozvoljen apsolutno nikakav nelegalan sadržaj i osoblje uklanja svaki koji se pojavi. Diskusija nije zločin. Vođenje foruma nije zločin. Ovde nema brojeva kreditnih kartica i bankovnih računa, pornografije, wareza niti ičega drugog što se u Sjedinjenim Državama ili međunarodnoj zajednici smatra nezakonitim. Svako navodno poslovanje između naših članova *nije naša stvar* i, ako se dešava, dešava se *izvan našeg*

foruma. Ovde ne odobravamo nikakve nezakonite radnje niti u njima učestvujemo.

Što je dublje zalazio u svet kardinga, to je njegova moralna mreža postajala sve više zamršena. Kao Iceman, nikad nije kupovao i prodavao kreditne kartice. Međutim, Vižn je stvorio i drugu onlajn personu, koja jeste trgovala njima. Sposobnost da razdvoje delove svoje ličnosti bila je među hakerima česta. Ponekad se čak činilo da Vižn veruje kako njegovi virtualni likovi razmišljaju i postupaju samostalno, te da su stoga moralno zasebne jedinke.

Kao Iceman, težio je da porazi svoje konkurente iz sveta kriminala, ali i policiju, kako bi se istakao kao neprikosnoveni gospodar sveta kardinga. To je zahtevalo strategiju na dva koloseka. Prvo je morao da identifikuje i raskrinka sve „tastere" (tajne doušnike – Confidential Informants, CI) i policajce infiltrirane u karderske forume. Drugo, morao je da porazi konkurenciju – sve ostale karderske forume koji su se nadmetali za nelegalnu trgovinu.

Mnogo pre no što je Tajna služba SAD uspešno zatvorila Shadowcrew, Iceman je identifikovao nekoliko njihovih ključnih članova koji su bili doušnici američkih i kanadskih kriminalističkih službi ili možda čak pravi policajci. Ljudi poput Icemana, koji se bave prevarama, znaju da moraju biti jednako vešti u prepoznavanju tog umeća kod drugih. Iskusni sajber lopovi i sajber policajci svesni su da ništa ne podstiče prerušavanje i obmanjivanje tako kao internet. Iceman je logično zaključio da je uočavanje „tastera" suštinski važan deo posla.

Kad bi ih otkrio, pisao je na forumima svoje čuvene otrovne tirade o njima. Neki članovi su došli do zaključka da se Iceman zaista previše buni. Može li biti da je glavni mozak CardersMarketa i sâm doušnik? Svakako je izgledalo tako kad je pokrenuo svoj master-plan za uništavanje konkurencije – seriju napada na suparničke karderske forume, namenjene da ih obori i prenese njihove obimne baze članova na svoj CardersMarket. Vižn uopšte nije krio svoje namere: sa sebi svojstvenom arogancijom, rekao je kako ne smatra da ostali kriminalni sajtovi, kao što su *scandinaviancarding.com* ili TalkCash „imaju ikakvog prava da postoje".

Kako bi istakao svoju superiornost, prvo je stvorio lažan digitalni trag, usled koga je izgledalo kao da se server CardersMarketa nalazi u Iranu, daleko izvan dosega policije, ali i ostalih kardera. Taj server se zapravo nalazio u Kaliforniji, ali Icemanova

sposobnost izvrdavanja bila je toliko dobra da je zaista sve redom ubedio da je baza sajta smeštena u Iranu. To je, prirodno, samo dolilo ulje na vatru glasina: je li Iceman agent iranske obaveštajne službe, sa zadatkom da zbuni policiju SAD i sakupi finansijska sredstva za svoje tajne operacije?

Ko god da je bio, bilo je jasno da misli ozbiljno. Uspešno je hakovao jedan po jedan suparnički karderski sajt i počistio njihove baze podataka, koje su obuhvatale sve imejl adrese i lozinke članova, zajedno s arhivom svih ikad okačenih postova. Zatim je sve te informacije integrisao u CardersMarket, da bi potom obrisao svu evidenciju s originalnog sajta.

Njegovi napadi su bili nemilosrdni – čak ni Rusi nisu bili pošteđeni njegovog gneva. Imao je petlje da hakuje *mazafaka.ru*, ikonski sajt koji je u srcu ruskih hakera zamenio CarderPlanet. Međutim, iako mu je ego povremeno zamagljivao rasuđivanje, savršeno je dobro znao da uništavanje ruskih sajtova onako kako je to uradio s onima s engleskog govornog područja ne bi bilo nimalo pametno. Neki od najbriljantnijih hakera na svetu su Rusi i Iceman ni najmanje nije želeo da ih provocira. Štaviše, posle obaranja Shadowcrewa, Rusi su vrlo brzo napustili karding žurku. To jest, otišli su – manje ili više masovno – sa foruma na engleskom jeziku. Vavilonske diskusije kriminalaca, doušnika, špijuna i policajaca na anglofonim sajtovima postajale su iritirajuće i počinjale da guše: smetale su poslovanju. Rizik kom su se izlagali bio je zanemarljiv, pod uslovom da se drže podalje od zemalja u kojima bi ih se mogle dokopati američke kriminalističke službe.

Tako su ruski hakeri osnovali niz foruma na kojima se govorilo isključivo ili uglavnom ruski, među kojima i *mazafaka.rs*. Američkim kriminalističkim službama je bilo mnogo teže da se tu infiltriraju, a i saradnja s ruskom policijom ili mnogo uticajnijim KGB-om ispostavila se kao krajnje teška. Prva linija odbrane kriminalnih hakera u Rusiji ili Ukrajini uvek je vazda promenljivi lokalni žargon. Premda neki policajci sa Zapada koliko-toliko barataju ruskim da mogu da razgovaraju na tom jeziku, mnogo je teže biti u toku dinamičnih promena jezika povezanog s popularnom kulturom, s kojima tek mali broj onih u Vašingtonu i Londonu uspeva da drži korak.

I dok su ruski sajtovi veselo terali dalje, do leta 2006. Iceman je ubio skoro sve svoje protivnike s engleskog govornog

područja. A kad bi primetio da neko od njih pokušava da se ponovo podigne, pokretao je razorni DDoS napad.

DDoS napadi pojavili su se kao najčešće korišćeno oružje u sajber svemiru. Bili su delo takozvanih botneta, sajber ekvivalenta *Invaziji kradljivaca tela* (*Invasion of the Body Snatchers*) holivudskom klasiku iz pedesetih godina prošlog veka. Virus „zarobljava" kompjuter, koji potom pada pod uticaj takozvanog komandno-kontrolnog servera. Virus na taj način zarazi hiljade kompjutera, koji se potom nazivaju zombijima i uživaju status bespilotnih letelica koje sprovode naređenja moćnog k-k servera. Pri tom nastavljaju da funkcionišu kao po svemu normalni kompjuteri. Obični korisnik nije svestan da je njegova mašina sada vojnik u ogromnoj Armiji digitalnih mrtvaca. Ako je posredi naročito aktivan zombi, nedužna žrtva će možda primetiti da joj je kompjuter pomalo spor, obično zato što je preopterećen ulogom nevidljivog pomoćnika u distribuiranju milijardi spam imejlova, bilo da je reč o reklamama za novu metodu uvećanja penisa ili vikodin, ili da sadrže novu kopiju virusa koja će zaraziti još više kompjutera.

Međutim, botnetima se umesto toga često nalaže da pokreću DDoS napade, u kojima svi zombiji u isto vreme dobijaju naređenje da pristupe određenom sajtu. Ako je sajt ili server meta DDoS-a, on jednostavno pada od naprezanja da opsluži toliki kompjuterski saobraćaj. Stranica se ukoči. Ukoliko je napad dovoljno jak, ukoči se ceo sistem.

Ti nemilosrdni DDoS napadi osigurali su da je zajednica hakera prestupnika počela da se gnuša Icemana zbog njegove arogancije. Međutim, njegova taktika potpirila je sumnje da on možda radi za federalce zato što su veliki deo njegovih žrtava činili hakeri i kriminalci.

Niko, međutim, nije mogao da ospori njegove rezultate i dobit, budući da je CardersMarket sad imao nekoliko hiljada članova, koji su svi i dalje aktivno kupovali i prodavali kreditne kartice, bankovne račune, viruse, identitete i koješta drugo. Do avgusta 2006. Iceman je postao glavni baja.

Ipak, nešto mu je i dalje bilo kost u grlu. Jedan kriminalni sajt nije hteo da umre. Kad god bi udario na njega, bilo tako što bi mu počistio bazu podataka i pobrisao sve fajlove ili tako što bi naredio svojoj armiji zombija da ga zbriše s Mreže, on se uvek

vraćao, poput onih smešnih debeljušnih lutkica koje se uvek usprave kad ih oboriš.

Bitka s DarkMarketom je počela.

16.
DarkMarket

Sajberspejs, 2005/08.

Dok su se frizirana kola spuštala zapadnim rubom Alpa, sunce se odbijalo od jedre površine Sredozemnog mora pojačavajući osećaj da će vikend biti fenomenalan. Grupa mladih Skandinavaca od dvadesetak i nešto koju je predvodio Recka, kralj švedskih kardera, skrenula je s autoputa A8 na Grand Korniš i potom se niz serpentine spustila niz planine do Monaka.

Jedna od najmanjih i najgušće naseljenih zemalja sveta, kneževina se većim delom prošlog veka prosto davila u vlastitom glamuru. Godine 1956. postavila je zlatni standard posleratne globalne „selebriti" histerije kad je Grejs Keli, jedna od najzanosnijih holivudskih princeza, udajom za princa Renijea, naslednika monegaškog prestola, ušla u pravu kraljevsku porodicu.

Sada, tačno pedeset godina posle venčanja stoleća u Monaku, grupa DarkMarketara naoružana riznicom retkog plastičnog blaga pripremala je kratki pljačkaški pohod na ovaj hram dekadencije. Ubrzo nakon što su prešli iz Francuske u Monako, na vidiku su se pojavile prve kockarnice. Te fabrike gotovine još od 1860-ih obezbeđuju budžet kneževine. Tamošnji živalj naziva ih „buđelarom Monaka" i one su razlog što Monegašani ne plaćaju porez. Zašto bi? Jednokrevetna soba u hotelu Monte Karlo bej staje 800 dolara za noć, na primer, a ako je gost može sebi priuštiti, tada očigledno može i da ubacuje nezamislive sume novca u sefove kockarnica. Rezultat – para kao blata.

Domaće stanovništvo se tako prosto kupa u novcu kojim se superbogati neštedimice razbacuju za stolovima za blekdžek i rulet. Gostujućim stanovnicima je često lako da se rastanu s tolikom gotovinom baš zato što je to novac koji bi im u zemlji u

kojoj oni ili njihov biznis provode najviše vremena otišao na porez državi. Budući da je Monako sigurna luka za izbegavanje poreza – a prema podacima poštovane Organizacije za ekonomsku saradnju i razvoj (Organisation for Economic Cooperation and Development, OECD), i za pranje novca – vlasti u ovoj krševitoj naseobini fiskalne slobode navikle su da posetiocima svoje male zemlje ne postavljaju pitanja o poreklu njihovih finansija.

Savršeno mesto, dakle, za grupu DarkMarketara naoružanih tucetom Centurion kartica American Expressa, legendarnim Crnim Ameksima, olimpskim božanstvima Doba plastike koja garantuju prijem putem specijalnih pozivnica samo trulim bogatašima sa Zapada, iz Japana, Hongkonga i sa Bliskog istoka. U Americi, naknada za pristup Centurion klubu iznosi 5000 dolara, posle čega se plaća godišnja naknada od 2500 dolara. No, u zamenu za to, Centurion obezbeđuje besplatne avionske karte, vrhunski nastojnički servis, lične asistente za kupovinu i članstvo u elitnim klubovima diskretno razbacanim po svetu, o kojima mi, stanovnici Planete kulučenja nemamo pojma.

Jesmo li pomenuli keš? Pokažite svoj Centurion i možete se od glave do pete umotati dolarima, evrima, funtama, švajcarskim francima ili jenima koje će vam blagajnik predati s diskretnim osmehom rezervisanim za osobe vašeg bogatstva i statusa. Jedan jedini Centurion bio bi skoro dovoljan za plaćanje otkupa za taoca kog su oteli somalijski pirati.

Nema ničega neobičnog u tome da grupa mlađarije s previše novca za sopstveno dobro dođe u Monte Karlo da troši, troši i troši novac sa svojih Centuriona – razmažena derištad su sasvim normalna pojava u tom okruženju. Bili su rešeni da do kraja iskoriste svojih dvanaest magičnih tokena. Prvo luksuzni hotel, potom kokteli i raskošna večera, a onda pravac Kasino. „Bila je to luda žurka", sanjalački se priseća jedan od njih. „Dve hiljade šesta bila je vreme kad se DarkMarket vinuo do neba." Za dva dana koliko su ostali u Monte Karlu, mladi karderi su preko svojih Crnih Ameksa podigli 400.000 dolara. I sami priznaju da su bili šokirani koliko je bilo lako. „Nisu ni trepnuli. Niko nam nijednom nije zatražio neka lična dokumenta i onda stekneš osećaj da ljudi stalno rade takve stvari."

Nisu samo Skandinavci uboli džekpot. Zloglasni ukrajinski karder Maksik zarađivao je stotine hiljada dolara preprodajom „dampova i fulova", brojeva kreditnih kartica zajedno s PIN-om i

onim trima ciframa na poleđini kartice. ChaO je u Turskoj stvorio pravu fabriku kriminalne aktivnosti unovčavajući klonirane kreditne kartice, prodajući „skimere" lopovima širom sveta kako bi mogli da samostalno kradu podatke s kreditnih kartica.

DarkMarket.com osnovan je maja 2005, ali je za prvih nekoliko meseci postojanja bio poprilično beživotan. U jesen iste godine, međutim, privukao je neke značajne likove s drugih karderskih foruma. Najenergičniji među njima bio je JiLsi, haker sa Sri Lanke, koji je već bio osnovao jedan sajt, The Vouched, i dosegao status moderatora na maloj ali uticajnoj engleskoj sekciji na *mazafaki*.

Nije prošlo dugo a JiLsi je postavljen za globalnog moderatora na DarkMarketu, samo jednu stepenicu ispod najvišeg statusa administratora. Zadao je sebi da uzdigne profil DarkMarketa. Imao je isti cilj kao Iceman sa sajtom CardersMarket – JiLsi je želeo da on bude priznat kao najjači kriminalni sajt na engleskom govornom području. Neumorno radeći iz internet kafea Java bin u severnom Londonu, do maja 2006. uspeo je da privuče stotine novih članova. Uglavnom su bili s engleskog govornog područja, premda je često navraćao i poveći broj Rusa.

Baš kad je sajt postajao popularan među karderima u celom svetu, njegovi prvobitni osnivači odlučili su da ugase DarkMarket, zato što su se bojali upada bezbednosnih službi. Jedan je čak brinuo zato što su postali previše uspešni. JiLsi i njegovi prijatelji želeli su da iskoriste ovu rastuću reputaciju i prosto su registrovali sajt kao *darkmarket.ws* (domen Zapadne Samoe).

Sad su zaista mogli da prionu na posao. Zajedno sa JiLsijem, DarkMarket dičio se sponzorstvom uglednog ruskog hakera koji je koristio ime Shtirlitz, veterana s CarderPlaneta, koji je delovao kao most između ruskih karding sajtova i DM-a.

Bilo je i drugih. Matrix001 je razgledao DM. Otkako je postao član Međunarodnog udruženja za unapređenje kriminalne aktivnosti, njegov ugled specijaliste za grafički dizajn je rastao. Nije bio impresioniran onim što je video – forum je bio spor i nezgrapan, a bezbednost nikakva. Poslao je administratoru JiLsiju nimalo uvijenu poruku, u kojoj je istakao da neprijatelji poput Icemana, usled neadekvatnog softvera, svakodnevno hakuju sajt. Ponudio se da instalira bolji sistem, što je JiLsi sa zahvalnošću prihvatio, i tako je Matrix započeo svoj uspon u hijerarhiji.

Pristizalo je još pomoći. JiLsi je vrlo brzo unapredio izvesnog Master Splyntra u moderatora na forumu. Master Splyntr je bio nadimak ozloglašenog poljskog spamera Pavela Kaminskog. Kao tipična adolescentska referenca, njegov nadimak odnosio se na pacova koji je obučavao Nindža kornjače borbenim veštinama u popularnom dečjem crtanom filmu. U znak poštovanja prema svom heroju i njegovom umeću, Master Splyntr je u zajednici hakera i spamera bio poznat i kao „sensei".

Pravi identitet Master Splyntra otkrila je tajanstvena britanska antispam organizacija, *spamhaus.org*. Poslovni ljudi, tekiji, bivši obaveštajni agenti i bog te pita ko još sačinjava taj tim koji vodi pravi krstaški rat sa ciljem da stavi na crnu listu sve velike igrače iz sveta spama, kardinga i dečje pornografije. Prečešljavaju digitalni svet u potrazi za „kvarnim" ISP-jevima, čiji se internet provajderi prave da ne vide kriminalne aktivnosti svojih klijenata. Kaminski je, izvestio je Spamhaus na svom sajtu, jedan pet najvećih spamera na svetu, odgovoran za ogromne količine neželjenih reklama za uvećanje penisa, vikodin i ostalo.

Zanimanje Spamhausa za Master Splyntra značilo je da je on obeležen i, kad je iz spaminga prešao na karding, njegove aktivnosti postale su predmet policijske istrage u pet zemalja. Kaminskog su povezivali i sa velikoprodajom malvera, virusa i trojanaca. Bio je poznat kao opak tip i JiLsi je u sebi bio oduševljen što je u vode DarkMarketa namamio tako krupnu ribu. Marljivo je kultivisao i Splyntra i Matrixa001. To se razvijalo u odličan tim, a kad se društvu priključio ChaO, turski kriminalni mastermajnd, DarkMarket je dobio neospornu auru uspešnosti.

Kad ga pogledaš, doduše, u njemu nije bilo ničega posebnog. Funkcionisao je potpuno isto kao forumi na kojima se diskutuje o opasnostima roditeljstva ili radostima pčelarstva. Pristup je bio teži zato što su članovi morali biti nominovani i potom provereni, ali to se retko ispostavljalo kao problem za one upoznate sa karding scenom i rešene da se učlane. Stvarni biznis – kupovina i prodaja – gotovo se nikad nije obavljao na forumu, iz bezbednosnih razloga. Forum je pre svega bio mesto gde se prodavci i kupci mogu sresti; proizvođači skiming uređaja su tu nalazili svoje tržište; onima koji su posedovali baze podataka s kreditnih kartica pružala se prilika da regrutuju tim za „unovčavanje" (ključni zadatak obilaženja bankomata i podizanja gotovine s računa). Međutim, o pojedinostima svakog posla skoro uvek se

dogovaralo razmenom privatnih poruka preko enkriptovanih ICQ mreža. Kad se postigne dogovor, dve strane su se vraćale na sajt, gde su podnosile zahtev za usluge garantnog servisa, gde su administratori obezbeđivali poštenu igru.

Forum je privlačio sve više članova i posao je prosto cvetao. Ključni pojedinci delovali su kao veza između ruskih kriminalaca i kardera sa Zapada, ali je JiLsi u isto vreme primećivao da se geografski krug proširuje. Turska je prerastala u važnu zonu sajber kriminala. Zajednice u Španiji i Nemačkoj rasle su velikom brzinom, dok su čak i francuski karderi – koji se, poput većine Francuza, prijatnije osećaju u internet okruženju u kom se govori francuski – brusili svoj engleski kako bi ušli u okršaj.

Dolazilo je zlatno doba DarkMarketa.

17.
Kancelarija

Kancelarija Renua Subramanijama bio je terminal u internet kafeu Java bin. Tokom prethodnih osamnaest meseci Renu je uglavnom radio na Mreži uz pozadinsku kakofoniju brušenja i škripe, budući da se skromni Java bin nalazi u senci stadiona Vembli – a stadion je tada prolazio kroz rekonstrukciju monumentalnih razmera, koja je sredinom 2006. već bila premašila i rok i budžet.

Kafe je gotovo po svemu bio nalik hiljadama drugih razbacanih po svetu. Njegovo okruženje nije bilo zdravo. Ugnežđen između salona za manikir po imenu Bowling Nail & Beauty i knjigovodstvene firme prilično musavog izgleda, posedovao je nekoliko vremešnih, glomaznih monitora i lepljivih tastatura povezanih s nepouzdanim kompjuterima s lažnom oznakom marke, očiglednih jeftinih kopija iz istočne Azije. Samo bog zna kakve su se sve aktivnosti odvijale iza klimavih drvenih pregrada što su delile prljave konzole.

Pognuti nad monitorima, adolescenti su satima igrali onlajn igrice, često s neverovatnim nivoom koncentracije; putnici pešaci s rancima na leđima sastavljali su zabavne imejlove prepune utisaka o novootkrivenim krajevima; radoznali tinejdžeri i frustrirani sredovečni muškarci surfovali su po čudnim porno sajtovima; mladi idealisti planirali su političke proteste zamišljajući da svraćanjem u ove anonimne lokale izmiču oku Velikog brata; dileri droge dogovarali su se o mestima isporuke i metodama pranja novca; a sajber kriminalci logovali su se na net da vide vrednost najnovijeg plena.

Osim lokacije u senci nedovršenog stadiona Vembli, Java bin je posedovao još nešto po čemu se izdvajao od ostalih. Naime, kompjuteri u internet kafeima obično su opremljeni samo ograničenom zaštitom od napada spolja. U njima ima virusa, trojanaca i ostalih digitalnih bakterija, baš kao što njihovi organski ekvivalenti nastanjuju bolnice s aljkavo održavanom higijenom.

Renu je, međutim, ozbiljno shvatao pitanje bezbednosti i ubedio je menadžera Java bina da na sisteme kafea instalira specijalni program zvani Deep Freeze („duboko zamrzavanje"). Taj program je vraćao čvrste diskove na prethodnu konfiguraciju, što je osiguravalo da mreža više nije mogla da „vidi" nikakav malver koji je možda daunloudovala u toku dana, čime je osujećivala delovanje svega zlonamernog i pojačavala Renuovu zaštitu.

Ako je Java bin bio Renuova kancelarija, ormarić za kartoteku koji je sadržavao tajne DarkMarketa sastojao se od minijaturne USB memorije. Renu je obično čuvao svoj hard disk doslovno na srcu. Po dolasku u kancelariju, uključio bi USB u neki od kompjuterskih terminala i počeo da radi na DarkMarketu.

Nakon što se uloguje, Renu bi nabacio svoju masku pirata i postajao JiLsi, jedan od osam administratora koji su upravljali DarkMarketom za vreme trogodišnjeg postojanja sajta. Ovaj tim, koji nikad nije brojao više od četiri člana istovremeno, bio je jedna od najuticajnijih jedinica na globalnoj sceni kardinga. Renuu to rukovodeće mesto nije donosilo neki poseban dodatni prihod, ali bio je to povlašćeni položaj koji je garantovao znatan ugled među hakerima i krakerima. Takođe, administratori su imali pristup velikim skladištima informacija i držali u rukama ključ virtualnog života i smrti – vlast da isključuju članove zbog stvarnih ili navodnih prestupa.

Uzvišeni položaj administratora imao je i dva velika nedostatka. Kao prvo, to je bio veoma težak posao, koji je redovno podrazumevao petnaest do sedamnaest sati svakodnevnog kucanja na tastaturi. Za te ljude nije bilo nedelje ni praznika – od njih se očekivalo da dežuraju sve vreme, 365 dana u godini. Master Splyntr je, na primer, uvek imao uza se mobilni telefon koji ga je upozoravao da je potreban nekom kolegi DarkMarketaru, i javljao se svaki put kad taj telefon zazvoni. JiLsi se žalio kako se uloguje u devet ujutru, a u deset naveče još sedi tamo. Posao je uglavnom bio dosadan i jednoličan: pratili su postove, kako bi bili sigurni da se članovi povinuju pravilima foruma i da se poruke ostavljaju na pravom mestu. Većinom se svodio na birokratiju i bio je uglavnom trivijalan i psihički zamoran.

Kao drugo, tim administratora je stalno pristupao unutrašnjim mehanizmima kriminalnih sajtova. Digitalni trag koji je to ostavljalo na Mreži bio je potencijalno mnogo vidljiviji od onog

koji je identifikovao obične članove, zbog čega su administratori bili primarni cilj sajber policajaca.

To je paradoksalno, budući da su „obični" članovi rutinski najviše zarađivali od DarkMarketa: administratori su se često izlagali najvećem riziku, a za najmanju finansijsku dobit. JiLsi i Matrix su za tri godine zaradili bednu sumu, dok je Master Splyntr naplaćivao samo za održavanje servera, usredsređen na druge delove svoje spaming imperije.

Zatim, tu je bio zanimljivi lik Shtirlitz, i to skoro od samog početka. Nadimak je aludirao na izmišljenog Maksa Ota fon Štirlica. U romanima Julijana Semjonova, Štirlic je bio visoki nacistički oficir koji je za vreme Drugog svetskog rata špijunirao za Moskvu. Okarakterisan kao ruski Džejms Bond, Štirlic se ukorenio u ruskoj svesti zahvaljujući popularnim filmovima iz sedamdesetih godina prošlog veka, zasnovanim na tim romanima. Ćutljiv ali izuzetno zgodan, Štirlic je u postkomunističkoj Rusiji ostao snažan patriotski simbol, zbog svoje neizmerne hrabrosti, inteligencije i nepokolebljive odanosti otadžbini.[24]

Poznajemo, dakle, sovjetskog špijuna Štirlica, ali ko je bio karder Shtirlitz (koji je transkribovao svoje ime s ruskog na engleski, pa otud dodatno „h")?[25] Je li i on bio agent KGB-a? Ili možda dvostruki agent, koji je radio za federalce ili Tajnu službu? Ili je bio vrhunski karder? Jedan član CarderPlaneta koji ga je upoznao opisao ga je kao muškarca „arijevskog izgleda, u kasnim dvadesetim godinama". Redovno je kupovao falsifikovane pasoše i izvesno vreme je živeo u Pragu, glavnom gradu Češke. Na CarderPlanetu opisivali su ga kao „dobrog i pouzdanog momka", ali su ostali karderi kasnije počeli da sumnjaju da se nije možda ugledao na svoj uzor iz sveta fikcije i preobrazio u jednog od najiskusnijih pripadnika američkih kriminalističkih službi.

Koji god da su bili njegovi stvarni ciljevi kao jednog od viših članova DarkMarketa, bio je sveprisutan ali tih, beležeći relativno malo aktivnosti. Isto tako, član koji se kasnije uključio u administraciju foruma, Lord Cyric, izgledalo je da uopšte nije

24 Ovaj književni serijal Semjonova pretočen je 1973. u seriju nazvanu *Sedamnaest trenutaka proleća*, po jednom od romana iz serijala, a snimljeno je i nekoliko filmova. Glavnu ulogu, lik ruskog špijuna infiltriranog u nemački vojni vrh, tumačio je Vjačeslav Tihonov. (Prim. prev.)

25 Ne samo „h", nego i „tz": nemačko Stierlitz se na ruskom piše fonetski, Штирлиц (Prim. prev.)

uključen u kupovinu ili prodaju. Obojica su bila prezauzeta nastojanjem da sve ide kako treba, uživajući za to vreme u bratstvu status legende.

Međutim, svako je imao svojih tajni, a neki uopšte nisu bili ono što su izgledali.

Ironično, onaj koji je najozbiljnije shvatao svoju bezbednost bio je u nekim aspektima najtransparentniji. To je bio ChaO. Taj turski kriminalac je relativno kasno došao na karderske forume. Za razliku od ostalih, on nije bio veteran sa Shadowcrewa ili IACAA, već se početkom 2006. pojavio kao da je pao s neba, kao vlasnik foruma zvanog *crimeenforcers.com*, elegantno dizajniranog sajta koji je ambicioznim sajber kriminalcima nudio svu moguću tehničku podršku. Bio je naročito poznat po svojim animiranim tutorijalima u kojima je glavnu ulogu imao ChaO, ali kao crtani lik, koji je vodio gledaoca kroz detaljni prikaz kardinga.

ChaO je koristio DarkMarket da promoviše *crimeenforcers* (plaćene reklame predstavljale su za forume važan izvor prihoda), a njegova sveprisutnost i neumorne poslovne transakcije ubrzo su prerasle u stvarni uticaj. DarkMarketu se pridružio u februaru 2006, a u roku od sedam meseci postavljen je za jednog od šefova.

Za razliku od svojih kolega, spadao je u onu retku sortu: gik s briljantnim zločinačkim umom. Njegova motivacija za prihvatanje vodeće uloge bila je jednostavna – mogao je da je iskoristi za unapređenje svog posla, distribucije uređaja potrebnih za finansijski kriminal, kao što su „skimeri" – aparati koji mogu da čitaju, skladište i šalju podatke s kreditnih kartica žrtava.

Međutim, kao što je to slučaj i s ostalim vodećim ličnostima DarkMarketa, ChaO-va priča se naposletku ispostavila kao mnogo složenija – ništa čudno za stanovnika Istanbula.

Ostavimo li po strani ovaj izuzetak, najuspešniji lopovi na DarkMarketu nisu pomagali u upravljanju sajtom. To su bili ljudi kao Freddybb i Recka, karderi iz Skantorpa i Švedske, koji su samo povremeno navraćali da obave posao i potom se danima, nedeljama, pa čak i mesecima nisu pojavljivali. Kriminalističke službe širom sveta uhapsile su u sklopu svojih sajber operacija mnogo više gikova nego okorelih kriminalaca.

Dirinčeći za svojim kompjuterima, četiri glavna menadžera bila su kolektivno odgovorna za četiri glavna zadatka. Za zaštitu servera i opšte održavanje bili su odgovorni Master Splyntr i Matrix001. Svakodnevne pretnje sajtu nisu poticale od policije nego

od suparnika i neprijatelja DarkMarketa, koji su se takođe nalazili u kriminalnom sajberspejsu, kao što je bio Iceman. Splyntr, Matrix i JiLsi su uzdisali svaki put kad bi među članovima izbila neka rasprava ili svađa. Splyntr se već navikao na obrazac, mada je postalo pomalo zamorno. Jedan karder bi optužio drugog za neki prestup, možda neosnovano, možda s pravom. Optuženi bi pobacao sve svoje igračke iz kolica i uskoro bi povređena strana rasporedila botnete s namerom da lansira DDoS napad. Desetine hiljada kompjutera pod zapovedništvom jedne komandno-kontrolne mašine zatražilo bi tada pristup DarkMarketu i tako oborilo sajt. Da se sve to dešava u fizičkom svetu, mrmljao je Splyntr *sebi u bradu, onda prosto odeš i razbiješ skota od batina. Međutim,* u virtualnom prostoru nemaš mnogo izbora sem da zatvoriš sajt i sačekaš da se napadač smiri ili ispregovaraš nekakav sporazum.

Posledica toga bila je da su administratori morali da prate sve sukobe koji su izbijali među članovima i pokušavaju da stišaju strasti pre no što kulminiraju. Prosečan sajber kriminalac ima manire šimpanze i jezik sicilijanske prodavačice ribe. Anonimnost je na internetu urodila suštinskim nedostatkom poverenja, čemu je svet kriminalaca naročito podložan zbog potencijalne pretnje od strane policije i utiska neranjivosti koji odaje ta anonimnost korisnika. Zbog toga uvrede na forumima poput DarkMarketa vrlo brzo eskaliraju u otvoreni rat. To je, uzgred, i jedan od aduta u rukama policije koja istražuje sajber kriminal – u zajednici koju izjedaju svakojake sumnje, onaj ko ume da čita između redova može da manipuliše sporovima u svoju korist.

O sudbini statusa članova unutar hijerarhije DM-a odlučivao je, normalno, tim administratora. Njih četvorica bi se izdvojila u privatnu sobu – forum kojem su samo oni mogli da pristupe – da porazgovaraju, na primer, o tome jesu li informacije o prodavcu ukradenih kreditnih kartica dovoljno pouzdane da mu se dodeli zavidna titula „proverenog dobavljača", a koja mu je omogućavala da bez ikakvih ograničenja prodaje kartice na DarkMarketu.

Administratori su, prirodno, neprekidno motrili na eventualno prisustvo sajber policajaca, da i ne govorimo o „ološu i deratorima" – kriminalcima koji su odbijali da se povinuju pravilima podzemlja.

Uočavanje „deratora" bilo je ujedno i ključni deo trećeg i najvažnijeg zadatka administratora – vođenja garantnog servisa koji je obezbeđivao poštenu igru u carstvu nepoštenja. Kao i na

prvom karding sajtu, CarderPlanet, uspešno vođenje garantnog servisa bilo je od presudnog značaja u preobražavanju DarkMarketa u najjači kriminalni sajt svog vremena. Garantni servis je vodio JiLsi, ali je njegov najvažniji arbitar bio ChaO.

Naposletku, administratori su morali budno da motre za slučaj da neko koristi sajt za distribuciju dečje pornografije ili kupovinu i prodaju droge i oružja. Razlog za to nije bila moralna indignacija već uverenje da će policija biti manje energična u svojoj poteri za njima ukoliko se ograniče na karding i krađu identiteta.

Prva polovina 2006. bila je za Renua i dobra i loša. Maler ga je poterao u februaru. Izašao je iz Java bina posle celodnevnog dirinčenja i uputio se da veče provede uz martel i krek. Kad se sutra ujutru probudio, shvatio je da njegov USB nije na uobičajenom mestu, siguran na njegovim grudima. Ostavio je prokletinju u kafeu!

Spopala ga je panika. Ušavši u Java bin, odmah je otišao kod menadžera da se raspita da mu ga neko nije dao. Menadžer je odmahnuo glavom. „Upravo si me stajao četvrt miliona funti!", viknuo je Renu, zaboravivši načas da je sam kriv za katastrofu. Bio je manje zabrinut za sopstvene ograničene finansije nego za novac i podatke deponovane u garantnom servisu.

Narednih nekoliko nedelja, JiLsi je pokrenuo operaciju popravka štete. Morao je da ubedi članove DarkMarketa koji su mu ukazali poverenje da im bezbednost nije ugrožena. U međuvremenu, u stvarnom svetu, Renu se mučio da plati rate za kredite kojima je pokupovao neke zapuštene nekretnine u severnom Londonu. DarkMarket je prosperirao, ali JiLsi se nije bogatio. Naprotiv, tonuo je u dugove i obratio se nekim „prijateljima" tražeći zajam. To što je bio begunac u sajberspejsu nije ga pripremilo za poslovanje s tim tradicionalnijim „podzemljem".

Čak i nakon što je izgubio USB memoriju, Renu je nastavio da se nesebično posvećuje DarkMarketu i njegovom napretku. Međutim, stres usled vođenja sajta polako je postajao preveliki. Pre svega, postalo mu je jasno da su se DarkMarket i CardersMarket upustili u borbu na život i smrt. Sajt je bio ranjiv, ali JiLsi je bio još ranjiviji i ponekad se osećao krajnje umoran od cele te rabote.

Iceman je intenzivirao svoje nasrtaje, zasipajući DarkMarket DDoS napadima i vatrom iz svih ostalih digitalnih oružja kojih je mogao da se domogne. Karderi širom sveta svrstavali su se uz

jedan ili drugi sajt, tvrdeći kako bi protivnik trebalo da se skloni i omogući dominaciju jednog megasajta. To je, štaviše, bio i Icemanov glavni argument: konkurencija u ovom slučaju nije poboljšavala efikasnost, već je samo dovodila do ogorčenosti.

U septembru 2006. nemilosrdni napadi dovodili su Renua do očajanja. Njegova zavisnost od kreka je u to vreme takođe postajala sve veća, što je bilo opasno za njegovu bezbednost – o zdravlju da i ne govorimo – ali i za bezbednost DarkMarketa.

Odlučio je da o napadima na sajt porazgovara sa Master Splyntrom, koji je u to vreme bio moderator, dve stepenice ispod JiLsija, koji je bio glavni administrator. Master Splyntr je odavno govorio da bi JiLsi trebalo da pusti njega, Kaminskog, da preuzme servere. Kaminski je tvrdio da je spremio mnogo bolje obezbeđenje i da će, ako preuzme taj resor, to umanjiti pritisak pod kojim se nalazi JiLsi.

Master Splyntr bio je JiLsijev rezervni izbor. Ponudu je prvi dobio ChaO, ali je Turčin odbio, nesumnjivo nimalo oduševljen nezahvalnim poslom održavanja servera. Niko drugi nije hteo da se prihvati i tako JiLsi nije imao izbora do da pozove Master Splyntra.

Kaminski je poziv primio početkom oktobra 2006, oko pola dvanaest uveče. „Moji serveri su spremni, JiLsi", rekao je. JiLsi više nije oklevao, srećan što će se rešiti barem odgovornosti za svoje ranjive servere. „OK. Idemo, onda!"

Možda predviđajući da im neće biti pravo, JiLsi nije konsultovao svoje kolege administratore pre no što je predao server Splyntru, mada se posle ispostavilo da niko nema prigovora. Brzo su se uverili da je odluka bila pametna – Splyntr se pokazao kao efikasniji menadžer servisa nego JiLsi.

Kaminski je održao reč: njegovi serveri bili su efikasni i bezbedni. I ne samo to: kad su svi pokušavali da ustanove gde se zaista nalaze serveri DarkMarketa (bilo kolege hakeri, policija, vojska ili obaveštajne službe), nisu ih mogli pratiti dalje od anonimnog servera u Singapuru.

Master Splyntr imenovan je za administratora. Saobraćaj na sajtu ponovo je počeo da raste. Svaki put kad bi Iceman hakovao DarkMarket i uništio mu bazu podataka, Master Splyntr bi ga u roku od dvadeset četiri sata ponovo podigao. I premda je Iceman neosporno bio najtalentovaniji tehničar u igri, njegova aroganci-ja je udaljila stotine kardera. DarkMarket je postao jači no ikad i

izgledalo je da ništa ne može da zaustavi njegov uspon do vrha. Međutim, Iceman je imao još jednog keca u rukavu.

18.
Podozriva priroda

Naizgled miran, Iceman je zapravo bio besan kao ris. Bio je izgubio pojam o vremenu. Moglo je biti tri ujutru, moglo je biti tri posle podne. Međutim, kad si zadubljen u veliku provalu koja ume da potraje satima, lako postaneš dezorijentisan. Većina opsesivnih hakera potpuno prestane da primećuje vreme i prostor. Kad bi Icemana obuzeo gnev, nije postojao stvarni svet – važne su bile samo zapovesti Nemeze, boginje osvete.

Sada se pojavljivala u nekoliko obličja. Prvi je bio El Mariachi, ogorčeni karder čiji je sajt, The Grifters, Iceman uništio. El Mariachi je sa digitalnih brda vikao kako poseduje neoborive dokaze o Icemanovom pravom identitetu saradnika FBI-ja. Tu optužbu je ponavljao i Lord Cyric, njegovo poslušno kuče, koji je povazdan kevtao i režao na karderskim forumima. Poput mnogih drugih, Iceman je prezirao Lorda Cyrica.

Žučne optužbe preletale su do jednog do drugog karding sajta. Bilo je ravno ratu između mafijaških klanova, s tim što niko nije bio potpuno siguran ko pripada kojoj porodici, ko je doušnik a ko federalac. Vladao je haos.

Međutim, kad je Iceman otkrio ono za šta je poverovao da je istina, sedeo je gotovo zabezeknut u svom udobnom stanu u centru San Franciska, koji su mu Džefri Normington i još jedan partner plaćali u zamenu za redovni priliv ukradenih brojeva kreditnih kartica. Odatle je, okružen komadima bajate pice i limenkama koka-kole, Iceman administrirao CardersMarket i opsesivno hakovao druge karderske sajtove. U oktobru je uspeo da upadne u samo srce servera DarkMarketa.

Počeo je ispitujući celokupan administratorski saobraćaj, a onda spazio neke IP adrese koje su mu delovale čudno. Svako može da potraži IP adresu i vidi gde se ona nalazi – koja kompanija ili pojedinac su povezani s njom, kao i ime matičnog provajdera internet usluga (Internet Service Provider, ISP). Jedna je bila registrovana na kompaniju pod nazivom Pembrook Associates.

Iceman je prečešljao Mrežu uzduž i popreko u potrazi za informacijama o njoj, ali nije našao ništa sem na sajtu koji je navodio spisak firmi. Tu su se nalazili naziv kompanije i njen telefonski broj. Potom je obavio obrnutu pretragu telefonskog broja i dobio adresu povezanu s njim: 2000 Technology Drive, Pittsburgh, PA.

To je bilo sasvim dovoljno da čak i Iceman zadrhti. Naleteo je na ovu adresu pre nekoliko nedelja, nakon što je jedan kolega s CardersMarketa pronašao na sajtu na šablon koji je obuhvatao skraćenicu NCFTA i tu istu pitsburšku adresu. Kad je potražio tu organizaciju, Iceman je otkrio da je reč o Nacionalnoj alijansi za obuku sajber forenzičara (National Cyber Forensic Training Alliance), kvazi-državnom telu koje pomaže raznim kriminalističkim službama SAD u njihovom radu na širokom spektru problema vezanih za sajber bezbednost.

Zaronjen duboko u svoj virtualni svet, Iceman je odjednom osetio ledeni dodir stvarnosti. Oduvek je podozrevao da policija vreba iza svakog ćoška, ali ovo je bilo nedvosmisleno – bio je ubeđen da nikako ne može biti greška. Nakon što je mesecima verovao kako je nedodirljiv, čovek koji vlada karding zajednicom, Maksa Vižna najednom je ophrvala zabrinutost.

Posle podužih konsultacija, trojica Icemanovih kolega s CardersMarketa – silo, c0rrupted0ne i dystopia – rešili su da kontaktiraju sa Matrixom001 sa DarkMarketa i saopšte mu svoje sumnje u vezi s IP adresom i FBI-jem, i isplaniraju šta će dalje. Matrix001 je bio jedini administrator za koga niko nije smatrao da je ni na koji način povezan s policijom, stoga su mu preko ICQ-a poslali dokaze o NCFTA i ulici Technology Drive u Pitsburgu, zajedno s jasnom porukom:

dystopia: odavno znamo za ovo, ali najzad imamo dokaz
dystopia: matrix, DM je zamka
dystopia: 100 %

c0rrupted0ne: potrudili smo se da prekinemo neprijateljstva i ako izađemo u javnost policija će se žestoko obrušiti na nas ali ako ne kažemo ništa odgovorni smo za sve one koje sjebu

siloadmin: srećno, ti si admin policijske zamke!

siloadmin: Pembrooke Associates Technology Dr Pittsburgh PA 15219. zvuči poznato ovaj 2000 Technology Dr?

Matrix je njušio prevaru. Po pravilu nije verovao nikom, ali bio je naročito sumnjičav kada su posredi bili cOrruptedOne i silo. CardersMarket je dugo postupao prema DarkMarketu s neobuzdanom agresijom, u nadi da će ga na bilo koji način uništiti. Ispitao je dokument i, uprkos tome što mu engleski nije maternji jezik, smesta uočio da je prepun grešaka.

matrix001: ovaj word dokument je lažnjak
matrix001: zar niko od vas nije primetio slovne greške u njemu?
matrix001: da, i u vrhu stranice se ne navodi kompanija ili neko drugo ime
matrix001: piše nacfta
matrix001: samo adresa
matrix001: da pomenem samo jednu slovnu grešku: piše se available, a ne avaliable[26]
matrix001: hoćete da nabrajam dalje?

Odgovor siloadmina bio je defanzivan, kao da je bio ljut na samog sebe zato što nije primetio slovne greške.

siloadmin: slušaj matrixe
siloadmin: znam da ovo sranje izgleda ko lažnjak, sa slovnim greškama itd.
siloadmin: ali to smo pronašli
siloadmin: nisam ga iz prsta isisao

matrix001: nijedna kompanija na svetu neće nikad objaviti ovakav dokument
matrix001: to je van svake pameti

Ovo je lako mogla biti nameštaljka, a razgovor je ubedio Matrixa da je upravo o tome reč. Optuživanje suparničkih foruma da su klopka, tajna policijska operacija, predstavljalo je uobičajenu praksu namenjenu da isprepada članove i natera ih da pređu na

26 Eng.: dostupno, na raspolaganju. (Prim. prev.)

konkurentski sajt. Ako članovi napuste DarkMarket, Matrix je bio ubeđen da bi ih Iceman i CardersMarket smesta regrutovali, što bi moglo da zapreti i samom postojanju DarkMarketa.

Zatim, silo, dystopia i cOrruptedOne su uporno - možda previše uporno - zahtevali da Matrix otvori fajl koji su mu poslali, komprimovani zip fajl poznat kao rar. Zip fajlovi važili su za neke od najozloglašenijih nosilaca trojanaca i bio je siguran da je taj osmislila ekipa s CardersMarketa kako bi s njegovog kompjutera isisala sve tajne DarkMarketa. Počeo je da se pita nisu li Iceman i njegove kohorte prešli na drugu fazu drskog plana koji je smislio FBI u nameri da zbriše DarkMarket.

Bilo je oko devet i petnaest ujutru tog hladnog novembarskog dana u centralnoj Nemačkoj, ali Matrix je znao da mora brzo da dela. Smesta je kontaktirao sa svojim kolegama administratorima DM-a i upozorio ih da se Iceman i njegove kohorte spremaju da potkažu DM:

matrix001: nisam daunloudovao fajl i otvorio ga, rekao sam im da mi rar ne radi
matrix001: kladim se da je bio trojanac
matrix001: a ako proverite informacije koje su dostavili, sve sam go lažnjak...
matrix001: Ali pročitajte sami...

19.
Doni Brasko

Pitsburg, oktobar 2006.

Specijalni agent Kit Dž. Mularski iz Sajber odseka FBI-ja bio je uzrujan, i to ne samo zato što su Stilersi igrali osrednje posle februarske senzacionalne pobede u Superboulu. Kao čovek koji je unapred kupovao sezonsku kartu za Hajnc fild, domaći stadion Stilersa, Mularski je oduvek priznavao da fudbal nije pitanje života i smrti – nego još važniji od toga. Međutim, desilo se da je ovog puta imao ozbiljnije probleme od fudbala.

Već mesecima je radio kao sajber Doni Brasko, zagnjuren u sve prostranije vode kriminala na Mreži. Istina, život mu nikad nije bio u opasnosti kao agentu Džou Pistoneu onda kad se pod imenom Doni Brasko uvukao u jazbine najjačih mafijaških porodica u Njujorku.[27] Međutim, Mularski je morao mnogo da se trudi dok nije nagovorio svog šefa da odobri tajnu operaciju u sajberspejsu, što se nikada dotad nije preduzimalo. Povrh toga, bilo je i skupo, a nosilo je sa sobom i veliku opasnost da se pročuje da je zapravo reč o zamci. Zbog toga su šefovi FBI-ja pratili svaki njegov potez kako bi predupredili eventualne propuste. Međutim, ovo što se upravo dogodilo nije bio propust. Ovo je bilo ravno čeonom sudaru u punoj brzini.

Trenutak nije mogao biti gori. Postigao je mnogo a da ga nisu provalili. Bio je na korak od toga da dobije pomoć nekoliko stranih kriminalističkih službi koje su bile rade da se uključe u njegovu davnašnju strategiju spektakularnog niza hapšenja širom sveta. Stvorio je i potom gajio lik, odabrao ime i priču koja uz

27 Agent FBI koji je sedamdesetih godina prošlog veka proveo šest godina u najvišim krugovima njujorške mafije, omogućivši tako hapšenje i zatvaranje preko dve stotine ključnih kriminalaca iz tzv. Pet porodica. (Prim. prev.)

njega ide, a taj plod mašte postao je za neverovatno kratko vreme stvarnost za mnoge globalne sajber lopove.

Sada mu je, međutim, zbog nepažnje kolege koji je na kompjuteru ostavio fajl s tragom zaglavlja Nacionalne alijanse za obuku sajber forenzičara, pretilo raskrinkavanje i kolaps izuzetno složene operacije.

To je ujedno bio i prvi pohod FBI-ja na sajber kriminal. Dotad su u sajber istragama dominirali Poštanski inspektorat i, pre svega, Tajna služba SAD. Negde oko 2004. postalo je jasno da je sajber kriminal jedan od najbrže rastućih sektora organizovane kriminalne aktivnosti u svetu. Provale u kompjutere organizacija, institucija i pojedinaca bile su sve češće. Najveći problem predstavljale su kreditne kartice, zbog ogromnog broja onih koje su bile nezakonito korišćene ili ukradene. Međutim, sad su i velike kompanije postale žrtve industrijske špijunaže, u kojoj su se njihove poslovne tajne krale i prodavale konkurenciji, što je bilo delo istih onih hakera umešanih i u prevare s kreditnim karticama. Cisco Systems je dozvolio da mu kineska konkurentska firma ukrade i kopira planove za jedan od njegovih najnaprednijih servera – dakle, čak ni kompanije koje bi trebalo da znaju sve o kompjuterskim mrežama nisu bile neranjive.

Nemaran pristup obezbeđenju kompjuterskih sistema, kako u vladi tako i u privatnoj industriji, počeo je da plaši Belu kuću, Kongres i Pentagon. Vladine agencije i ministarstva bili su najvećim delom nesvesni svoje ranjivosti ili u toj meri pritisnuti brojnim napadima lansiranim protiv njih da su zarivali glavu u pesak u nadi da će problem možda prosto nestati.

Za Pentagon, međutim, tako nešto nije dolazilo u obzir. Oni su, naime, imali pune ruke posla pokušavajući da se izbore s posledicama serije neprekidnih napada na kompjuterske sisteme Ministarstva odbrane (službeno nazvanim „Titan Rain"), poteklih iz Kine i namenjenih da iskopaju sva poverljiva dokumenta nepromišljeno ostavljena u nedovoljno dobro zaštićenim fajlovima.

Velike banke još nisu uspevale da dođu sebi posle takozvane pvv pošasti (pin verification value tj. potvrda verodostojnosti PIN koda), koja je za vreme aktivnosti Shadowcrewa stajala Citibank i Američku banku desetine miliona ukradene gotovine; premda su one taj problem rešile, stotine drugih banaka još su sipale novac iz svojih bankomata u ruke kardera.

Jednom rečju, haos.

Posledice toga nije bilo teško zamisliti. Neće proći dugo, a ogromne količine novca poreskih obveznika biće preusmerene u srodne probleme sajber kriminala, sajber industrijske špijunaže i sajber ratovanja. Nijedna kriminalistička služba koja drži do sebe neće hteti da se odrekne svog dela. S tačke gledišta FBI-ja, Tajna služba SAD imala je da se počasti trima četvrtinama bogatog budžetskog kolača. Ta služba, koja je iznedrila prve sajber policajce, još se baškarila u slavi stečenoj obaranjem Shadowcrewa i naravno da je želela da potvrdi svoj primat na tom potpuno novom polju.

FBI, najveća i najmoćnija kriminalistička služba u Americi, imala je drugačiju zamisao. Njenom direktoru Robertu Mileru bilo je veoma stalo da se uključi u istrage sajber kriminala, kako bi agencija dobila finansijska sredstva, ali i zato što je odigrao važnu ulogu u nastojanju da FBI postane manje policija a više domaća obaveštajna agencija. Plan Mularskog nije obuhvatao samo hapšenje kriminalaca već i prikupljanje informacija. Ova promena pravca u vrhu službe doprinela je da se prigovori nekih šefova prevaziđu i Mularski, koji je bleštavom prezentacijom potkrepio svoj zahtev da pokrene odvažnu tajnu operaciju, dobio je odobrenje koje je priželjkivao. Stoga, kad je Iceman upro prstom u njega, nije se samo Operacija DarkMarket našla na rubu propasti. Ako ovaj poduhvat propadne, s njim u nepovrat otići će i budući dolari iz budžeta i navodna sposobnost FBI-ja da vodi sajber operacije. Ramena Mularskog pritiskao je težak teret.

U prvi mah je pao u očajanje. Igra je gotova, pomislio je, a njegov marljivi tim moraće da pripremi ponižavajuće objašnjenje za šefove, od kojih će neki mrmljati: „Lepo smo vam rekli!" Međutim, jedan od razloga što je FBI odabrao Mularskog za svoj program obuke agenata bilo je pre svega to što je umeo brzo da misli onda kad je gusto. Prošlo je samo nekoliko minuta dok nije rešio da se neće predati bez borbe.

Životne okolnosti porodice Mularski u stopu su pratile sudbinu Pitsburga u XX veku. Njegov čukundeda je 1892. kupio u Hamburgu kartu za brod, s kog je u Baltimoru sišao s jednim dolarom u džepu. Kit možda jeste tipičan Amerikanac, ali etnički identitet brojnih evropskih zajednica u gradu ostao je snažan – poljski, u slučaju Mularskog.

Raštrkane među skromnim drvenim kućama, art deko bioskopima i plesnim dvoranama pitsburškog danas pitoresknog Saut

Sajda, nalaze se crkve i klubovi mnogih slovenskih zajednica – češke, poljske, srpske, slovačke, ukrajinske i drugih – koje su gravitirale prema ovom strategijski lociranim gradu u zapadnoj Pensilvaniji. Početkom XX veka, Andrij i Julija Vorhola, bračni par Rusina iz ruralnih predela severoistočne Slovačke, emigrirali su u Pitsburg, izbacili „a" s kraja svog prezimena i rodili jednu od najuticajnijih figura u umetnosti XX veka.

Moćni čelični mostovi i putokazi koji još pokazuju prema železničkoj stanici Norfok end vestern samo su neki od podsetnika na vitalno važan doprinos Pitsburga globalnoj ekonomskoj dominaciji Amerike u XX veku. Čelik iz tih fabrika preobražavao se u krstarice, avione, automobile i industrijska postrojenja širom sveta. Prošle su decenije otkako su crni oblaci, što su kuljali iz hidre koja je proizvodila čelik, poslednji put obavili grad tamom šireći otrovne čestice koje su nekad bile uzrok najviše stope plućnih bolesti u Sjedinjenim Državama.

Nakon što je diplomirao istoriju na Dukejnovom univerzitetu, Mularski se našao među onima što su osamdesetih godina prošlog veka pobegli iz grada. U to vreme, tamo nije bilo više ničega. Njegov otac kao da je bio reinkarnacija Vilija Lomana.[28] Jedan od prvih koji su na sopstvenoj koži osetili sve lošiju sreću giganta koji je lagano padao na kolena, Mularski stariji je 1970-ih otpušten sa radnog mesta trgovca, posle čega nije uspevao da nađe novi posao. Porodica je živela nesigurno, samo od plate Kitove majke, koja je radila kao sekretarica.

U vreme Kitove mladosti populacija Pitsburga je opala za jednu trećinu. Pošto nije nameravao da posmatra grad kako propada, on se sa svojom mladom ženom preselio u Vašington. Zaposlivši se u velikoj firmi koja je posedovala lanac prodavnica nameštaja širom zemlje, Mularski se ispostavio kao talentovani menadžer i trgovac. Na prvi pogled, reklo bi se da posao menadžera prodaje ima malo zajedničkog sa sajber kriminalom, ali tehnike koje je naučio u kompaniji dale su mu čvrste osnove za rad sajber policajca u FBI-ju.

U srcu sajber kriminala leži „društveni inženjering" – umeće da ubedite nekoga da uradi nešto što objektivno nije u njegovom interesu. Kako, pita se varalica, da ubedim svoju metu da mi oda

28 Protagonista dramskog komada Artura Milera *Smrt trgovačkog putnika* (1949). (Prim. prev.)

svoju lozinku? Da otvori imejl u čijem je kodu skriven trojanac? Ili da čak uopšte uključi kompjuter?

Postoje neke očigledne opcije koje stoje na raspologanju sajber lopovu. Dva oprobana i dokazana metoda jesu besplatno daunloudovanje muzike i pornografija. Seksualni nagon je jedan od najjačih – mora da bude, pošto se, u evolutivnom smislu, nalaženje partnera često ispostavljalo kao opasna rabota. Da bismo zadovoljili svoje seksualne želje, spremni smo da se izložimo neverovatno velikom riziku, što su proizvođači kompjuterskih virusa brzo shvatili. Obećanje golih grudi neretko je sve što je potrebno da bezazleni korisnik klikne na link koji će potom daunloudovati destruktivni malver u njegovu mašinu. Ako ima sreće, moguće je da će ga uistinu preusmeriti na sliku, mada je to bedna naknada za to što predaje sve tajne na svom desktopu bezličnom kontroloru ko zna gde. Nije slučajnost što je jedan od najuspešnijih virusa koji se širio putem imejla imao „volim te" kao naslov poruke.

Mada menadžeri prodaje nisu skloni da šire viruse, oni su, baš poput sajber lopova, uspešni inženjeri ljudske duše. Njihov zadatak je da ubede potencijalne mušterije da ulože novac u artikle koje ne žele ili im nisu potrebni. „Prodati nešto što imaš nekome ko to želi – to nije biznis", primetio je jednom prilikom gangsterski kralj Mejer Lenski. „Ali prodati nešto što nemaš nekom ko to ne želi – to jeste biznis." U najmanju ruku, menadžeri prodaje kadri su da ubede mušterije da kupuju skuplju robu. Tako je novopečeni agent Kit Mularski, kad je primljen u tek formirani Sajber odsek FBI-ja, sa sobom doneo nešto izuzetno cenjeno – sposobnost da obrlati, da bude duhovit, da saoseća, nagovara, mami i zavodi. Za jednog policajca, bio je vrlo ubedljiv kriminalac.

Do 2000. Pitsburg se preobrazio. Oduvek je imao tu sreću da dobija ogromne filantropske legate. Posvuda po gradu mogu se videti znamenitosti s imenima Karnegija, Hajca i Melona, kolosa američkog industrijskog napretka s kraja XIX i početka XX veka. Za svoj oporavak posle kolapsa velikih čeličana, grad može da zahvali i ulaganju u informatiku i kompjutersku tehnologiju na Univerzitetu Karnegi Melon (Carnegie Mellon University, CMU), svrstanom među dvadeset najboljih visokoškolskih ustanova u svetu.

Univerzitet, koji je osnovao veliki industrijalac škotskog porekla Endru Karnegi, počeo je kao tehnički fakultet, da bi se

1967. spojio s Melonovim institutom za industrijsko istraživanje. Za vreme sumornih osamdesetih i devedesetih godina prošlog veka, CMU je proučavao odumiranje Pitsburga i istraživao kako da ga vrati u život. Univerzitet je bio dobro poznat i po svom radu u oblasti kompjuterske bezbednosti. Pored Masačusetskog tehnološkog instituta i Silicijumske doline, Pitsburg se takođe ispostavio kao jedan od malobrojnih „rasadnika" gikova u Sjedinjenim Državama, sa specijalistima naklonjenim rešavanju problema bezbednosti.

Stručnost CMU objašnjava mnogo toga o novom Pitsburgu, uključujući i pojavu (1997. godine) Nacionalne alijanse za obuku sajber forenzičara, neprofitne organizacije koja je, uz podršku banaka i raznih korporacija, težila da spoji profesionalce iz univerzitetskih krugova, privatni sektor, kriminalističke službe i intelektualce, s ciljem da preduzmu nešto u vezi s rastućom nebezbednošću kompjuterskih mreža. To je i razlog što se Kit Mularski početkom dvehiljaditih vratio kući i počeo da radi iza neupadljivih staklenih zidova poslovne zgrade u ulici 2000 Technology Drive.

Dok je zurio kroz jedan od prozora na četvrtom spratu, bio je svestan da je gotovo isključivo odgovoran za ovu operaciju FBI-ja. Radio je s odličnim timom, ali on je bio taj koji je ubedio šefove, uprkos njihovoj velikoj sumnjičavosti, da mu daju zeleno svetlo. Na kocki nisu bili samo ugled federalaca i pitanje dela budžetskog kolača – nego i njegov posao, zaboga.

A onda se prisetio šta mu je istinski polazilo za rukom: prodaja. Ili, još bolje, društveni inženjering.

Kad se na BBS-ovima[29] kriminalaca pojavila vest da DarkMArket pripada federalcima, pribrao se i podsetio sebe da samosažaljenje još nikom nije pomoglo. Morao je smesta da pokrene protivnapad. Prišao je Grendelu, možda najtajanstvenijem od svih DarkMarketara. *Grendel je u stvarnom životu radio za potpuno legitimnu i vrlo sofisticiranu kompaniju za obezbeđenje kompjutera u Nemačkoj, ali je svoje usluge – uz plaćanje pouzećem – istovremeno nudio glavnim sajber kriminalcima.* DarkMarket je zavisio od njegovog VPN-a, koji je gotovo u potpunosti garantovao anonimnost – ali je Grendel otišao i dalje od toga, tako što je

29 Eng.: Bulletin Board System: „oglasna tabla", uobičajen je engleski izgovor Bi-Bi-Es. (Prim. prev.)

konstruisao četiri *„ljuske"* („shell"), softver koji može da učini korisnika nevidljivim.

Grendel je uspeo da iz ljusaka izvuče prethodne autentične logine, u kojima se nigde nije pominjao Pembrooke Associates. Mularski se ponosno pohvalio svim članovima CardersMarketa i DarkMarketa da je to njegov VPN servis, te da je jedini koji je mogao da ispovrti login sa Pembrooke Associates... Iceman. Posluživiši se svojim umećem prodaje, „Nemeza" Mularski je skrenuo reflektore sa sebe i uperio ih pravo u oči Icemanu.

Šlag na torti bile su štamparske greške na papiru sa zaglavljem koje je primetio Matrix001. Iceman je bio poznat po tome što je sve koji su ga iznervirali zasipao neosnovanim optužbama, a za vreme njegovog upravljanja CardersMarketom, skoro svi su ga u ovom ili onom trenutku iznervirali. Među njima je imao malo prijatelja. Isto tako, ideja da se Iceman vratio nekadašnjoj ulozi tajnog doušnika federalaca ponovo je uhvatila korena – a Mularski je svom snagom potpirivao tu tezu.

Iceman ne samo da nije uništio DarkMarket već je postigao sasvim suprotno od toga. Sajt je iz cele priče izašao jači nego ikada pre i sada su ga gotovo svi priznavali kao najjači svetski kriminalni karding sajt na engleskom govornom području. Domišljatost Mularskog sprečila je katastrofu.

20.
Lukavi plan

JiLsi je rastao kao kvasac. CardersMarket i Iceman su još bili na nogama, ali su se teturali od protivudaraca što su usledili posle otkrića o DarkMarketu kao policijskoj zamci. Većina kardera je sada (pogrešno) verovala da je CardersMarket policijska zamka, a da je DarkMarket čist. Posledica toga bila je da je DarkMarket ponovo počeo da raste ka svojih konačnih dve hiljade članova.

Razume se, još je bilo glasina da među administratorima DarkMarketa možda nije sve onakvo kakvo izgleda, ali kardera podleglih psihologiji čopora dotad je već bilo najmanje isto onoliko koliko i „vukova samotnjaka" iz pionirskih dana sajber kriminala. Čopor se okrenuo protiv Icemana i stao na stranu DarkMarketa.

U decembru 2006. DarkMarketari su funkcionisali kao dobro podmazana mašina. JiLsi je bio ponosan na svoj uspeh – najzad je postao poštovani član porodice, dobijao je priznanja za svoj nesebičan i efikasan rad. Sastavio je odličan tim: Matrix, Master Splyntr i ChaO bili su prvoklasni administratori i svi članovi su imali poverenja u njihov garantni servis. Shtirlitz i Lord Cyric osiguravali su podršku i kredibilitet. Brzo su uočavali deratore i prevarante, i s tim samoživim ološem obračunavali su se po kratkom postupku kad god bi ovi izronili iz septičke jame sajberspejsa. Članovi su sve više poslovali između sebe i profit je počeo da raste ka onome iz zlatnih dana Shadowcrewa i CarderPlaneta.

Od obaranja Shadowcrewa prošlo je više od dve godine i ustalio se osećaj samozadovoljstva. „Vukovi samotnjaci", koji su sada činili manjinu na forumima, nikad nisu spustili gard. Pažljivo su vodili računa da se ni na koji način ne inkriminišu. Recka, švedski kralj bankovnih prevara, savesno je izbegavao trgovanje američkim kreditnim ili debitnim karticama, jer bi time odmah privukao pažnju američkih kriminalističkih službi; sa Šveđanima i ostalim Evropljanima mogao je da izađe na kraj, ali se brižljivo starao da Amerima ne gura prst u oko.

Mnogi karderi, međutim, pogotovo oni mlađi, bili su aljkavi što se tiče mera bezbednosti i izbegavali su da koriste enkripciju u svojim ICQ četovima, a nisu valjano održavali ni VPN i sisteme tunelovanja kako bi maskirali svoje IP adrese.[30] Mularski je pak u Pitsburgu neumorno sastavljao bazu podataka, uz pomoć programa koji je sam napravio a koji je bio u stanju da ukazuje na aktivnosti pojedinih kardera – čitao je njihove poruke, logovao se na njihov ICQ i IP adrese i, tamo gde je bilo moguće, povezivao to s računima u E-Goldu.

Korisnici ove ustanove za digitalnu valutu nisu znali da vladine agencije uživaju puni pristup arhivi E-Golda, omiljenom metodu kardera za međusobni transfer novca od februara 2006. To je usledilo pošto je Daglas Džekson, osnivač te institucije, uhapšen u Floridi pod sumnjom da se njene usluge koriste za pranje novca. Malo je sajber kriminalaca, međutim – možda nijedan – sabralo dva i dva u pogledu E-Golda. Rusi su se klonili takvih firmi sa sedištem na Zapadu a registrovanih u Belizeu; više su voleli WebMoney, sa sedištem u Moskvi, izvan dohvata zapadnih kriminalističkih službi.

Naoružan ovim sve obimnijim dokazima, Mularski je potkraj jeseni 2006. stupio u kontakt s policijom u brojnim evropskim zemljama. Razgovarao je s Agencijom za krupni organizovani kriminal u Ujedinjenom Kraljevstvu, sa Saveznom policijom u Nemačkoj, a kasnije i s regionalnom policijom u Baden-Virtembergu.

Kontaktirao je i sa OCLCTIC u Parizu, nedavno formiranom i prozaično nazvanom Centralnom službom za borbu protiv kriminala u oblasti informacione i komunikacijske tehnologije (L'office central de lutte contre la criminalité liée aux technologies de l'information et de la communication). Naišao je na pomalo hladan prijem. Francuska policija generalno rado sarađuje sa Sjedinjenim Državama, pogotovo u oblastima kao što su terorizam i sajber kriminal, ali u francuskom društvu još je duboko ukorenjena tradicionalna podozrivost prema Americi i njenim namerama u Evropi. Svaka vlada za koju se čini da „šuruje" sa SAD u opasnosti je da izgubi simpatije glasača, pa zato upozorava svoje organe da budu obazrivi kad posluju s vašingtonskim agencijama.

30 Tunelovanje je najvažnija komponenta tehnologije virtualnih privatnih mreža i predstavlja prenos paketa podataka namenjenih privatnoj mreži preko javne mreže. Ruteri javne mreže nisu svesni da prenose pakete koji pripadaju privatnoj mreži i VPN pakete tretiraju kao deo normalnog saobraćaja. (Prim. prev.)

Šef OCLCTIC-a, Kristijan Agrum, smatrao je apsurdnim to što se on i njegovi agenti, kad god zatraže pomoć kompanije kao što je Microsoft, izlažu riziku da izazovu negodovanje uz predvidljive optužbe kako je policija pod šapom velikih američkih korporacija. Bio je, međutim, svestan činjenice da ne možeš istinski početi da se boriš protiv sajber kriminala ukoliko ne ostvaruješ određeni stepen saradnje s kompanijama poput Microsofta. Artikulisan i oštrouman analitičar političkog minskog polja koje okružuje internacionalni policijski posao, Agrum se pomirio s tim da ni političari ni javnost u Francuskoj nemaju pojma o sajber kriminalu i onome što je potrebno da bi se on porazio. Izgledalo je da se većina Francuza zanosi mišlju kako je moguće boriti se s transnacionalnim kriminalom i obuzdavati ga a da pri tom ne prelaziš državnu granicu, pogotovo ako kriminalac o kom je reč ne govori francuski.

Mularskog je, međutim, čekao još veći šok od dobro poznatog problema galskog antiamerikanizma. OCLCTIC, rečeno mu je, već nekoliko meseci sarađuje s Tajnom službom SAD na slučaju povezanom sa... DarkMarketom. U toku je bila paralelna istraga, a on o tome nije imao pojma. Štaviše, Tajna služba SAD bila je krajnje nesklona da podeli bilo kakve informacije u vezi sa svojom istragom. Nekoliko meseci pre toga, šef Odseka za krivične istrage Tajne službe svedočio je pred Kongresom da su, zahvaljujući bliskoj saradnji sa „drugim federalnim, državnim i lokalnim kriminalističkim službama... u stanju da obezbede sveobuhvatnu mrežu razmene obaveštajnih podataka i resursa, kao i tehničku ekspertizu". Zaboravio je da to kaže i timu koji je istraživao DarkMarket, budući da su oni odbili da otkriju FBI-ju čak i na koga ciljaju. Situacija je pretila da postane komplikovana, kako za sajber policajce, tako i za sajber lopove.

Većini DarkMarketara (sem onima koji su sarađivali s Mularskim) kriminalističke službe su u to vreme bile u sporednom planu. Umesto toga, želeli su da potvrde nadmoć svog sajta tako što će dokusuriti Icemana. JiLsi je uzeo na sebe da zada smrtonosni udarac. Ako uspe, to će biti njegovo najveće dostignuće i ugled će mu znatno porasti. Pored toga, bilo mu je više nego dosta stalnih Icemanovih prepada, koji su mu stvarali beskrajni dodatni posao; a žučna retorika, Icemanov zaštitni znak, takođe je počinjala da mu ide na živce.

JiLsijev plan je bio jednostavan. Otvorio je anonimni imejl nalog, koji je koristio za slanje poruka Icemanovom internet provajderu. Upozorio je taj ISP da je CardersMarket, kome je on davao hosting, kriminalni sajt čiji su vlasnici umešani u veliku prevaru s kreditnim karticama. Kad je Iceman otkrio odakle se šalju potkazivački imejlovi, upotrebio je JiLsijevu lozinku, MSR206 (naziv legendarnog uređaja za kloniranje kreditnih kartica, koji su koristili svi dobri karderi) i – dok si rekao „keks" – upalilo je. Iceman je saznao da ga je JiLsi popljuvao pred njegovim vlastitim ISP-om. To je bilo neoprostivo. JiLsi je zaista prekoračio granicu koju nijedan (ne)pošteni karder nikad ne bi smeo da pređe, bez obzira na to koliko su odnosi postali loši: ocinkario je pripadnika bratstva. Što je još gore, uhvaćen je na delu.

Iceman je ovo razglasio na sva zvona. Vrlo brzo, saznao je i ChaO.

Svi su bili još nervozni zbog bujice optužbi kojima ih je Iceman zasipao mesecima. Jesu li im federalci za petama? I ne samo to već, ako jesu: „Jebote, ko sarađuje s njima?", kako je to formulisao jedan od administratora DM-a. Iceman, Splyntr, cOrruptedOne ili Silo s CardersMarketa; Shtirlitz, zagonetni „Rus"; ili možda novi moderator DarkMarketa, Lord Cyric? Ili neko drugi?

Dve osobe koje do tog trenutka niko nije optužio da sarađuju s policijom bili su Matrix001 i JiLsi. Potonjeg su povremeno (ne bez razloga) optuživali kako je nesposoban. Ali saradnja s policijom? Nikad. Iceman je u svojim hakerskim pohodima već odavno doznao JiLsijevu lozinku. Međutim, sad su je izgleda svi znali. Pojavile su se sumnje da je neko treći ubacio trojanca na JiLsijev voljeni USB i da sada prati svako slovo koje ovaj pritisne na tastaturi, i tako saznaje najveće tajne DarkMarketa. Ili možda JiLsi nije onaj za koga se izdaje... možda je nekako povezan s misterioznom kompanijom iz ulice Technology Drive 2000 – Pembrooke Associates?

Nekoliko dana pre Božića 2006. Jilsi se, kao obično, ulogovao na DarkMarket da proveri saobraćaj. Nije se dugo zadržao, izlogovao se i otišao da se pozabavi problemima u svom stvarnom životu. Posle podne se vratio. *„Korisničko ime: Jilsi"*, otkucao je. *„Lozinka: MSR206."* Mašina je isti sekund odvratila: *„Pogrešno korisničko ime ili lozinka."* Pretpostavivši da je ukucao neko pogrešno slovo, JiLsi je automatski pokušao ponovo. Rezultat je bio isti. Zatim je probao još ko zna koliko puta.

Nije bilo nikakve sumnje: JiLsi, duhovni otac i glavni administrator DarkMarketa, bio je isključen sa svog sajta. Uspaničen, pokušao je da se uloguje na *www.mazafaka.ru*. Ni govora. The Vouched – još jedan od njegovih sajtova – zabranjen pristup.

Nije prošlo dugo a JiLsi je drhtao obliven ledenim znojem. Nikada dotad nije spoznao tako bolan pad. Oteli su mu ceo njegov život – ili barem jedino što mu je istinski značilo. Bio je ljut, povređen i potresen. Ko je to uradio i zašto? Odreagovao je tako što se prepustio anestetičkim svojstvima martela propraćenog lulom kreka. Bol je popustio na jedno veče i noć, ali JiLsi se probudio još nesrećniji nego juče.

Naposletku je uspeo da uspostavi ICQ kontakt sa ChaO-m. Razgovor ga je ostavio potpuno ošamućenog. „Znamo da radiš za Skotland jard i Odsek za haj-tek kriminal", rekao mu je ChaO. „Tvoja odluka da ocinkariš Icemana bila je konačni dokaz za to. Znamo da sarađuješ s policijom. Isključen si sa svih sajtova."

JiLsi je ostao bez teksta. Sve za šta se toliko trudio nestalo je za tili čas i sad je bio žrtveni jarac. Šta sad? Kuda? Beznađe i nespokoj, JiLsi, beznađe i nespokoj.

Deo V

21.
Dronovo zaveštanje

Kalgari, Alberta, 2006.

Dron je još od vremena kad se oglašavao na sajtu Shadowcrew dobijao samo najsrdačnije preporuke za svoj rad. „Juče posle podne dobio sam Dronov skimer", postovao je jedan zadovoljni kupac na DarkMarketu. „Proveo sam veče isprobavajući ga i stvarno sam vrlo impresioniran. Dron isporučuje prvoklasni proizvod, u potpunosti vredan vašeg vremena i novca."

Dron je držao reč. „Isporuka je bila brza, pakovanje diskretno", pisao je dalje autor posta. Međutim, ono što je Drona učinilo tako popularnim nije bilo efikasno otpremanje robe već odlična tehnička podrška zbog koje su kupci ponovo dolazili kod njega. „Dakle, briga o korisnicima, po mom mišljenju to je ono po čemu se Dron izdvaja. On svojim kupcima redovno šalje apdejte, a kad god sam mu poslao imejl s nekim pitanjem, odgovor je uvek stigao u roku od dvadeset četiri sata. Impresivno, nema šta."

Umnogome zahvaljujući internetu, kultura potrošačkih prava i očekivanja prodrla je konačno i u svet kriminalaca. Ako prodavac *zavrne* kriminalca na internetu, ovaj će mu vrlo teško ući u trag i primeniti tradicionalni metod izražavanja nezadovoljstva zbog loše usluge – fizičko nasilje. Umesto toga, kriminalci koji na Mreži trguju ilegalnom robom moraju da se nadmeću ko će ponuditi bolju uslugu.

U nekim drugim vremenima, Dron bi se brzo uzdigao do vrha. Tačno je da je još u petnaestoj prekinuo školovanje, ali zato je posedovao preduzetnički dar ujedinjen s kreativnom crtom. Nakon što ga je otac naučio kako da preko interneta igra na berzi deonica, naišao je na kriminalne forume i, kao dvadesetčetvorogodi-

šnjak, učlanio se u proleće 2004. na Shadowcrew, najuspešniji prethodnik DarkMarketa.

Međutim, njegova najveća veština ležala je u urođenom daru za tehniku. Počeo je od nule i sâm naučio da dizajnira i izrađuje skimere za dva najpopularnija tipa bankomata u svetu. Bile su to složene, zamršene naprave, vredne svaki cent od 5.000 dolara za koliko ih je prodavao (normalno, za kupovinu veće količine davao je popust). Ne samo da je mušterijama odgovarao na pitanja već je proizvode slao s uputstvom za upotrebu, odgovarajućim softverom i besplatnim USB kablom.

Koliko ozbiljno shvata svoj posao, otkrivala je i njegova biblioteka. Pored *Document Fraud and Other Crimes of Deception* stajale su *Holograms and Holography* i *Secrets of a Back Alley ID Man*. Međutim, možda najvažnija od svih bila je knjiga *Methods of Disguise* (u prevodu: Metode prerušavanja). Kad je navraćao u neki od brojnih internet kafea u svom mestu, odakle je upravljao svojom prodajom i marketingom na Mreži, Dron je najčešće nosio crnu bejzbol kapu i crni sako. Međutim, kad je odlazio u poštu ili „unovčavao" kreditnu karticu kao uplatu za neki svoj skimer, radije je nosio crvenu kapu i plavu vindjaknu.

Tajna služba Sjedinjenih Država je Drona prvi put uočila kroz značajno prisustvo na sajtu Shadowcrew. Razume se, administrator tog sajta, Cumbajohnny, bio je doušnik Tajnog servisa. Dron, međutim, nije pripadao Cumbajohnnyjevom VPN-u, glavnom sredstvu preko kog je Tajna služba pratila aktivnost članova. Nije se nalazio u Sjedinjenim Državama, niti je bio laka meta. Otud nije bio prioritet. Međutim, Tajna služba nije zaboravila Drona. Umesto toga, počela je da gradi odnos sa njim.

Iako mlada i zelena u poređenju s Poštanskim inspektoratom SAD, Tajna služba ima najduži istorijat borbe protiv kriminala. Formirana je 1865, ali ne zato da pruža oružanu zaštitu predsedniku SAD – to je bio jedan od glavnih odgovora Kongresa na ubistvo predsednika Makinlija 1901. godine. Prvobitna i stalna svrha agencije bila je da uočava, istražuje i potom traži podizanje optužnice protiv svakoga za koga se ustanovi da je proizvodio ili distribuirao falsifikovani novac. Ubrzo pošto je osnovana, Kongres je zadužio agenciju i za istrage finansijskih prevara.

Posle Drugog svetskog rata, Bretonvudski sporazum postavio je Sjedinjene Države za nepobitnog lidera privrede Zapada, a dolar kao odabranu valutu u kojoj su se čuvale rezerve u kapitalističkom

svetu. Mada su Sovjetski Savez i Kina odbacivali supremaciju dolara, obema komunističkim supersilama je, bez obzira na to, bilo veoma stalo da nagomilaju što više zelembaća. U svetu u kojem je većina vlada čvrsto držala na uzdi protok stranih valuta preko svojih granica, sveprisutnost dolara kao oblika plaćanja umnogome je povećavala privlačnost izdavanja falsifikovane valute SAD.

Rezultat je bila internacionalizacija operacija Tajne službe, budući da su lupeži i vlade širom sveta težili da se obogate odnosno da podriju moć Amerike štampajući svoje sopstvene dolarske novčanice. Gde god da čitate ovo, možete se pouzdati u to da se negde relativno blizu nalazi operativac Tajne službe. Međutim, iako ruka agencije seže daleko, postoje određene izolovane tačke do kojih čak ni ona ne može da se pruži – 1990-ih, na primer, svetom se raširio *superdolar*. Vlada SAD veruje da su te partije neverovatno vernih ali ipak lažnih novčanica od 100 dolara potekle iz štamparskih presa u Severnoj Koreji – jedne od malobrojnih oblasti izvan dosega „ljudi u crnom".

Primanje metka umesto predsednika i jurenje prefriganih, svim bojama premazanih dolara već su dovoljno težak posao, ali Kongres je 1984. zatražio dalju ekspanziju aktivnosti Tajne službe, koja će obuhvatati i istrage prevara s kreditnim i debitnim karticama i falsifikovanim dokumentima, i kompjuterskih prevara.

Naredne dve decenije, organizacija koja je, na neki način, najtajnija američka kriminalistička služba, specijalizovala se i za sajber kriminal, što je dovelo do razvoja operativnih sposobnosti bez premca. Međutim, Tajna služba zapošljava samo 6.500 ljudi. Nasuprot tome, FBI broji 30.000 zaposlenih. Nedavno je Tajna služba SAD pripojena Ministarstvu za nacionalnu bezbednost, što je ranilo njen ponos. Naime, ove dve agencije se baš ne mirišu. Da li zbog kompleksa niže vrednosti Tajne službe ili kompleksa više vrednosti FBI-ja, teško je reći – po svoj prilici je po malo od oboje. U svakom slučaju, imaju dugu istoriju sitničavih sporenja, što utiče na glavna operativna pitanja.

Posle obaranja sajta Shadowcrew, Tajna služba je rešila da neguje vezu sa Dronom, koji se potkraj 2005. priključio DarkMarketu, gde je njegova reputacija prodavca skiming uređaja porasla tolikom brzinom da je uskoro pokrenuo vlastiti sajt, *www.atmskimmers.com*. Mesecima je filijala Tajne službe u Bafalu mukotrpno nastojala da utvrdi Dronovo boravište. Ovaj dobavljač je koristio izraelski imejl servis Safemail jer je znao da ta

kompanija blokira IP adresu pošiljaoca, što je značilo da mu primalac ne može ući u trag. Do prodora u istrazi Tajne službe konačno je došlo u januaru 2006, kad je Safemail pristao da otkrije Dronove IP adrese nakon što se zahtev TS SAD silom probio kroz usporeni krivično-pravni sistem Izraela. Kako se ispostavilo, Dron je koristio više kompjutera lociranih na širem području Kalgarija u kanadskoj naftonosnoj provinciji Alberti.

Sledećih osamnaest meseci ispostavilo se kao naporno razdoblje za detektiva Spensera Frizela iz policije Kalgarija. Filijale Tajne službe u Bafalu i Vankuveru slale su mu IP adrese koje su dobijale od Safemaila svaki put kad bi tajni agent razmenio imejl sa Dronom. Te adrese su uvek pripadale ovom ili onom internet kafeu. Kad bi ga detektiv konačno locirao, ptičica bi dotle već odletela. Dok nije počeo rad na ovom slučaju, detektiv Frizel nije imao predstavu da u Kalgariju ima tako mnogo internet kafea niti koliko su popularni. Osećaj da traga za iglom u plastu sena postajao je sve jači.

Mesecima je izgledalo da Dron nasumično bira internet kafee. Jednog dana bi se pojavio na jednom mestu, sutradan pet kilometara dalje. Ponekad se činilo da je sasvim nestao iz Kalgarija, izazivajući strah da je otišao da se nikad ne vrati. Međutim, uvek se vraćao i, posle nekoliko meseci, Frizel je došao do važnog otkrića. Stavljajući pribadače na mapu, uočio je da se svi Dronovi internet kafei nalaze blizu stanica lokalnog voza u Kalgariju, na liniji koja ide od Somerseta do Kroufuta. Takođe je primetio dve ili tri prodavnice u koje je Dron, izgleda, voleo da zalazi.

To je značilo da ima dovoljno informacija da zatraži tim za praćenje. Naišao je na već uobičajene prigovore na koje nailaze svi sajber policajci u svetu. Ko su žrtve u Kalgariju? Koje dokaze imaš o prometu ostvarenom kriminalnom delatnošću?

Frizel je dobio odobrenje koje je tražio, ali samo na ograničeno vreme i s vrlo malo ljudi. Generalno, kad bi iz Tajnog servisa dobio dojavu da je Dron onlajn, poveo bi sa sobom onoga ko se nađe u kancelariji i uputio se negde duž linije lokalnog voza.

Detektiv iz Kalgarija je duže od godinu dana junački obavljao ovaj zadatak, lagano sužvajući krug osumnjičenih sve dok nije bio ubeđen da ima pravog čoveka. Ono što nije znao bilo je da se nalazio na prvim linijama šire operacije Tajne službe koja nije obuhvatala samo Drona nego i veći broj meta u Evropi. Tajna služba SAD kontaktirala je sa SOCA u Londonu i OCLCTIC u Parizu.

„Mi tako radimo", rekao je portparol Tajne službe Edvin Donovan. „Uvek se trudimo da maksimalno dobro sarađujemo s policijama iz celog sveta. Obratimo se agenciji koja se bavi ovom vrstom kriminala i kažemo da je meta taj i taj – i, dabome, razmena informacija je od ključnog značaja u ovakvim slučajevima."

Tajna služba je, dakle, razmenjivala informacije s policijom u Britaniji, Kanadi i Francuskoj. Međutim, grupa agenata s kojom ih još uvek nisu razmenjivale bile su njihove kolege u FBI-ju. Očigledna netrpeljivost između dveju američkih agencija izazvala je zbunjenost kod Evropljana – na kraju su Francuzi sarađivali s Tajnom službom, Nemci sa FBI-jem, a Britanci su učtivo balansirali između njih. Ovo je delovalo prilično ironično, budući da su jedini ljudi na svetu koji su znali da su se FBI i Tajna služba nameračili na istu osobu, JiLsija, pripadali stranim policijskim snagama, Agenciji za krupni organizovani kriminal u Londonu. Postalo je i gore – službenici SOCA shvatili su da obe službe zapravo drže pod istragom tajne agente konkurentske agencije, smatrajući ih osumnjičenim kriminalcima. Naposletku je jedan visoki britanski zvaničnik diskretno obavestio vlasti u Vašingtonu da bi FBI i Tajna služba, barem dok traje istraga, trebalo da ostave svoje razlike po strani.

22.
Dečko, baš si ga uprskao

Baden-Virtemberg, 2007.

Bilo je prijatno veče početkom maja, premda Matrix001 tog časa nije primećivao da je već uveliko proleće. Spoljni svet je nestajao dok su mu se usta sušila, a oči još jednom preletale preko imejla.

Prisluškuju ti fiksni telefon.
Na tragu su ti panduri u UK, Nemačkoj, Francuskoj... Sakrij dokaze.
Upozori ostale... Panduri znaju da je matrix001 detlef hartman iz ajslingena...
Imaš samo nekoliko nedelja pre no što panduri u UK i Francuskoj krenu u akciju...
Upozori sve kardere do kojih možeš da dođeš.

Šta sad ovo znači? Od koga je? Ponovo je pogledao adresu pošiljaoca: *auto432221@hushmail.com*. Bila je po svoj prilici nasumično generisana. I bilo je nemoguće identifikovati išta o autoru poruke, osim da, izgleda, tečno govori engleski.

Matrix je odlučio da se posavetuje sa svojim kolegama administratorima DarkMarketa i dvojicom drugih poverljivih ljudi. Upitao ih je šta misle o ovome. Njihovi odgovori bili su čudno mlaki, u nekim slučajevima gotovo ravnodušni, puka upozorenja za njega da motri šta se dešava.

Kit Mularski u Pitsburgu je pak bio sve samo ne ravnodušan. Odlomci imejlova koje su on i ostali agenti dobijali od Matrixa značili su samo jedno: negde je procurelo. A ako je informacija preneta Matrixu, ko je još upozoren? Teško da je trenutak mogao

biti gori, jer je FBI već nekoliko meseci planirao prvi talas hapšenja u operaciji DarkMarket. Bilo je dovoljno gadno što su morali da se bakću s nimalo kooperativnom Tajnom službom. Nemačka policija iz pokrajine Baden-Virtemberg čula je da njihove francuske kolege pripremaju niz hapšenja vezanih za DarkMarket, ali francuska policija ih je ignorisala, rekavši kako njihovo prisustvo u Parizu, na sastanku sa SOCA iz Britanije i Tajnom službom neće biti potrebno.

Anonimni *hushmail*[31] poslat Matrixu izazvao je među istražiteljima zebnju koja ih mesecima nije napuštala. Morali su da saznaju da li je curenje informacija bilo rezultat nemara ili ih je neko namerno odao, ili je možda neki haker prodro u jednu od kompjuterskih mreža istražiteljskog tima. Kad god bi nešto pošlo naopako, na površinu bi izbila sumnja da se u njihovim redovima nalazi izdajnik. Moral nije mogao a da ne opadne.

Pokušaji Mularskog da koordinira prva hapšenja nisu tekli lako. Svaki sajber policajac se pribojava da će se, ako jednog prevaranta uhapse pre ostalih, vest da se dešava nešto gadno raširiti po forumima kao šumski požar i da će mete jednostavno nestati. Otud i opsesivna tajnovitost Tajne službe...

Čekaj malo, pomislio je Mularski, verovatno je i procurilo baš odatle – iz Tajne službe! Pažljivo je razmislio o mogućim krivcima: a) Tajna služba; b) neko iz njegovog tima, u šta je čisto sumnjao zato što je bezbednost FBI-ja bila maksimalno pojačana otkako je Iceman primetio umešanost federalaca; c) SOCA je znala za Matrixa, ali su Britanci oduvek bili najćutljiviji od svih; i d) naravno, Nemci – ali jednostavno nije imao dovoljno iskustva kada je o njima reč, mada je naslutio pomalo zategnute odnose između regionalne policije u Štutgartu i uprave savezne policije u dva sata udaljenom Visbadenu, a i jedni i drugi su znali za priču o DarkMarketu?... Nije umeo sa sigurnošću da kaže.

To nagađanje je, međutim, privremeno moralo da padne u drugi plan. Prva briga Mularskog bila je da stupi u kontakt sa Frankom Ajsmanom iz regionalne policije u Štutgartu i popriča s njim o istrazi o Matrixu pre no što mladi Nemac zbriše. Štutgart je odlučio da je vreme da se slučaj ubrza i Ajsman mu je saopštio kada planiraju hapšenje. To je pak stvorilo probleme policijama u Londonu, Kalgariju i Parizu, koje su se na londonskom sastanku

31 Imejl servis koji, između ostalog, nudi PGP-enkriptovan saobraćaj elektronske pošte i sakriva IP adresu u zaglavlju poruke. (Prim. prev.)

početkom aprila bile konačno dogovorile da svoje osumnjičene zaskoče istog dana – 12. juna. SOCA se i dalje osećala pomalo neprijatno zato što je Tajna služba motrila na JiLsija još od vremena Shadowcrewa. I federalci i Tajna služba želeli su da ga se dokopaju.

Međutim, Matrix nije zbrisao. Umesto toga, njegovi četovi i imejlovi koje je presretala nemačka policija nagoveštavali su da ga onaj *hushmail* uopšte nije prepao. Možda je odluka da ubrzaju Matrixovo hapšenje bila preuranjena?

Desetog maja, tačno nedelju dana posle prvog imejla, dobio je još jedan. Ovog puta je stigao s adrese *auto496064@hushmail.com*, a auto496064 bio je malčice ljut:

> Dečko baš si ga uprskao.
> Naša mreža dala je vama nemačkim karderima pošteno upozorenje, a šta vi uradite? Pričate s jebenim FBI-jem!
> Toliko ste glupi da zaslužujete mardelj.
> Međutim, presreli smo komunikaciju između FBI-ja i nekog švabe koji sebe naziva „iceman". Jedan pandur koji se lažno predstavlja bacio je udicu i samo čeka da prodate/kupite nešto pa da vas upeca. Još nemamo ime. Ali možda ćete moći da nam pomognete da ga provalimo.
> I učini sebi jebenu uslugu. Dok ne budemo znali ko je taj tajni policajac, ne kupuj ništa ni od koga.
> Pošto ste bili tako prokleto pametni pa rekli FBI-ju da smo ih provalili, možda udare ranije! Obriši sve sa svog kućnog kompjutera, čak i ako je enkriptovano, jebote, i koristi *samo* internet kafiće.

Matrix je odbio da poveruje u ovo i ignorisao je poruku. Pripisao je to nekakvoj drugoj zakulisnoj igri, sličnoj onima kojih se sećao iz one rabote s Icemanom. Ali zato su policajci poludeli. Ovog puta je program koji je nadzirao kompjuter Detlefa Hartmana pokupio imejl kad ga je ovaj otvorio. Frank Ajsman (za koga je tajanstveni auto496064 greškom pomislio da je „iceman") prosto nije mogao da poveruje da neko prati svu komunikaciju na DarkMarketu. Među policajcima je zavladao strah da je hakovana čitava istraga DarkMarketa i da loši momci znaju o slučaju sve što i oni.

Mularski se takođe šokirao. Međutim, primetio je jednu važnu anomaliju – autor anonimnog imejla je možda potpuno tečno govorio engleski, ali nije bio Amerikanac, zato što je reč usluga pisao sa „u".[32] Ko je taj?

32 Engleski izraz za uslugu različito se piše u britanskoj i američkoj varijanti tog jezika: *favour* odnosno *favor*. Slovo „u" u toj reči značilo je da je autor Britanac ili neko kome engleski nije maternji jezik (udžbenici i priručnici se najčešće zasnivaju na britanskoj varijanti). (Prim. prev.)

23.
Udešena matrica

Dvadeset deveti maj 2007. Počinjao je još jedan utorak u Ajslingenu, jednoj od bezbroj nepoznatih nemačkih varošica u kojoj pokvareni semafor ili zalutala krava umeju mesecima da budu glavna vest i čiju rutinu retko kad išta remeti. Život u Nemačkoj budi se sat ili dva ranije nego u Britaniji ili Americi. U pola sedam ujutru mnoštvo ljudi je već krenulo na posao i usput navraća u lokalni kafić Čibo. Tu razmenjuju ono malo tračeva uz kafu, neprivlačno zalivenu kondenzovanim mlekom, kojoj ukus popravljaju kremasti kolači ili *weggle* s dimljenom šunkom (rolnica od testa na gotovo nerazumljivom dijalektu koji se govori u Švabiji).

Ipak, dan je bio predodređen da bude nesvakidašnji za Ajslingen, jer je u njega imao da stigne XXI vek. Negde na pola puta niz Ulicu H., Detlef Hartman se izvlačio iz kreveta maglovito svestan da je imao na pameti nešto važno. Dok mu se izmaglica u mozgu još razilazila, proverio je svoj *hushmail* nalog da vidi ima li nekih enkriptovanih poruka i pretražio svoj sajt da proveri jesu li potrebne neke popravke. Sve je bilo u redu.

Zatim se setio. Njegovi roditelji su se vraćali s odmora u Austriji. Stanje opšte uzbune.[33] On i brat imali su samo jedan dan da sve počiste i srede. Sasušeni špageti prianjali su za tanjire kao industrijski cement; pepeljare s brdima opušaka ležale su razbacane među praznim pivskim limenkama, flašama i neraspoznatljivim komadima odeće – tipičan spomenik koji sagrade dečaci u tinejdžerskim godinama kad ostanu prepušteni sami sebi. Detlef je odlučio da se na brzinu istušira pre no što počne da sređuje kuću i upravo se brisao kad se oglasilo zvonce na vratima. Doviknuo je bratu da otvori.

Detlefova iznerviranost što ga gnjave tako rano ujutru – tek je bilo prošlo pola deset – porasla je za stepen kad mu je brat iz

33 Eng.: *Action stations* – opšti signal posadi ratnog broda da verovatno ili sigurno predstoji bitka s neprijateljskim snagama, te da svi zauzmu svoja mesta. (Prim. prev.)

prizemlja viknuo nešto o nekakvoj isporuci i kako je potrebno da se potpiše. Silazeći niz stepenice, Detlef se pripremao za raspravu s poštarom zato što je došao na pogrešnu adresu. „Hajde već jednom", nestrpljivo mu je dobacio brat drhtureći na promaji dok se Detlef približavao kroz predsoblje.

„Onaj se nedozvoljeno parkirao", pomislio je Detlef sa sebi svojstvenim okom za detalje kad je ugledao crni kombi napolju na ulici. Ispred vozila stajala je poštarka, u uniformi koju je Detlef mogao da opiše samo kao ceremonijalnu. Kravata joj je bila zategnuta u mali čvor, a na glavi je imala krutu šapku. Držala se vrlo ozbiljno.

Poštarka se gotovo naklonila pružajući Detlefu jednom rukom koverat formata A4 a drugom hemijsku olovku. Dok je posezao za olovkom, skoro teatralnim pokretom povukla se korak unazad. „Šta se kog đavola događa...?" Međutim, pre no što je Detlef stigao da završi misao, na njega su skočila četvorica ljudi i našao se potrbuške na zemlji, s rukama na leđima. „Uhapšen si", povikao je jedan, dok je u kuću pokuljalo nekoliko policajaca koji su se kao niotkud stvorili tu. Detlef je još uvek ležao, obučen samo u donji deo pižame. Padala je kiša i bilo je hladno, svega desetak stepeni iznad nule. Nečija čizma pritiskala mu je vrat na ledeno tlo, dok mu se kabl kojim su mu vezali ruke urezivao u kožu. „Zaboga, šta se ovo dešava?", mrmljao je stalno i iznova, osećajući se kao da je upao na snimanje nekog drugorazrednog filma.

Deset minuta kasnije sedeo je preko puta detektiva Franka Ajsmana iz badenvirtemberške LKA (Landeskriminalamt Baden-Württemberg, Nacionalna policija Baden-Virtemberga). Policajac je smrknuto odmeravao lom u kuhinji, epicentru tinejdžerskog haosa. „Gospode, ovde kao da je pala bomba", primetio je.

Roditelji su im na godišnjem, objasnio je Detlef. „Jasno mi je", promrmljao je Ajsman sebi u bradu.

Nekoliko narednih minuta, policajac i uhapšeni sedeli su ćuteći. Čulo se samo cvokotanje Detlefovih zuba. Ulazna vrata su još bila otvorena i, posle onog kratkotrajnog boravka na kiši, telesna temperatura mu je padala. Sa sprata je dopro uzbuđen uzvik: „Kompjuteri su još u pogonu!"

Detlefu je najzad sinulo šta se dešava. Uprkos hladnoći i zbunjenosti, razmišljao je brzo i zamolio detektiva da ga pusti da nešto obuče. Nije bio sasvim neiskren: bilo mu je strašno hladno.

Ajsman je oklevao. Važi, složio se naposletku, upozorivši ga kako time krši pravila, ali da će mu ipak dozvoliti da se obuče.

U Detlefovoj sobi, Ajsmanov kolega stajao je ispred kompjutera kao da čuva gol, spreman da zaštiti mašinu od svakog diranja. Dok se Detlef mučio da navuče majicu, sapleo se, zgrabio kabl i izvukao utikač iz zida. Brujanje je prestalo. „Sranje, sranje!", viknuo je policajac. „Kompjuter se ugasio." U sobu je utrčao Ajsman. „U redu, to je to. Sad je gotovo – to je poslednje što si zadugo uradio." Odvukao je Detlefa nazad niz stepenice u kuhinju. Ajsman mu je gurnuo pod nos list papira ispisan pravničkim jezikom, ali jedino čega se Detlef seća jeste ono što je bilo dopisano slobodnom rukom: *„... osumnjičen za formiranje grupe za organizovani kriminal."*

Mada je bio besan na Detlefa, detektiv Ajsman mu je dozvolio da nakratko popriča s bratom. Detlef mu je rekao da ne brine, da će sve biti u redu. Brat nije odgovorio ništa, ali ga je gledao kao da je pomerio pameću. Naposletku, pre no što će ga izgurati iz kuće, Ajsman je upitao Detlefa želi li da ponese nešto sa sobom. „Možete li da mi kažete šta će mi biti potrebno?", odvratio je Detlef, pomalo zbunjeno. „Ovakvo nešto mi se još nije dogodilo."

Dok je na putu do policijske stanice zurio kroz prozor, u mislima se vratio na ona dva anonimna imejla koja je primio pre nekoliko nedelja. Gde mu je bila pamet? Zašto nije odreagovao? Međutim, koliko god je razmišljao, Detlef nije bio istinski siguran šta je uopšte mogao da uradi. On nije bio okoreli kriminalac koji na raspolaganju ima sigurne kuće i mafijašku mrežu. Bio je đak, mlad i prilično naivan. Jedva da je uopšte znao šta je to zločinačko udruživanje, a kamoli da bi mogao biti deo nečega takvog.

Kad su se patrolna kola zaustavila ispred velike bele zgrade na kraju primereno nazvane Ulice Ašperger u četvrti Štamhajm u Štutgartu, glavnom gradu Baden-Virtemberga, Detlef je još razmišljao o svemu tome. Da je pogledao ka jednom od prozora na četvrtom spratu, video bi ćeliju u kojoj se 1976. obesila Ulrike Majnhof, harizmatična predvodnica nemačke levičarske terorističke grupe koja je delovala 1970-ih.

Štamhajm je posle toga pretvoren u isključivo muški zatvor. Međutim, Detlefa je tamo uvela žena stražar. Čim su zatvorenici ugledali ženu, podivljali su, dobacujući iz ćelija na sav glas prostote kojima su opisivali šta bi sve voleli da joj urade.

Detlefov strah od novih okolnosti rastao je sa svakim korakom. Kako se dečko iz ugledne porodice iz srednje klase našao u ovakvoj situaciji? Gimnaziju je završio s odličnim ocenama i spremao se da upiše fakultet. Roditelji su ga obožavali i bili su mu zahvalni što im pomaže oko troje mlađe braće i sestara. Sad je bezazleni dečko iz Ajslingena bio u Štamhajmu, najzloglasnijem zatvoru u celoj Nemačkoj. Nakon što su mu naložili da skine odeću i pretražili ga, čuvari su mu dali preveliko zatvorsko odelo, ali ne i obuću. Njegova nova pižama bila je tako velika da ga je podsećala na pantalone za pecanje. Stigla je i hrana, ali njemu još nije dopiralo do mozga da je tu došao da ostane. Bio je u šoku. Malo po malo, shvatio je da je ovo poslednja etapa malog putovanja koje je započeo pre pet godina. Bilo je to samo dan posle njegovog dvadesetog rođendana.

24.
Francuska veza

Budući da su prestale da razgovaraju jedna s drugom, dve američke agencije su paralelno pokrenule svoje prepade na DarkMarket. Uz prisustvo Tajne službe, detektiv Spenser Frizel uhapsio je Drona u Kalgariju četiri dana pre operacije Matrix u južnoj Nemačkoj, koju je podržavao FBI.

Frizel je nedeljama sužavao krug „dežurnih krivaca" posećujući bezbrojne internet kafee iz kojih je Dron radio. Naposletku je izdvojio dvadesetšestogodišnjaka neupadljivog izgleda koji se kretao naokolo menjajući svoje tri „neformalne" uniforme. Meta je živela u pristojnom stanu u centru Kalgarija, naravno, zgodno lociranom nedaleko od stance lokalnog voza.

Međutim, ni Frizel niti agent tajne službe nisu bili potpuno spremni za ono što ih je dočekalo. Osumnjičeni, Nikolas Jele, imao je oko stotinu skiming uređaja u fazi proizvodnje. Da ih je sve prodao, to bi mu donelo 500.000 dolara, zajedno sa stotinama blanko plastičnih kartica spremnih za kloniranje i hologrami spremnih za falsifikovanje. Razume se, puko posedovanje ovih uređaja nije bilo prestup samo po sebi, ali je Frizel uspeo da ustanovi da je Jele za vreme trajanja istrage – nešto manje od dvanaest meseci – zaradio oko 100.000 dolara od prodaje skimera.

Jedno je kad kriminalistička služba uhapsi osobu osumnjičenu za kriminalnu aktivnost na Mreži. Prikupljanje dokaza dovoljnih za podizanje optužnice je već nešto sasvim drugo. Virtualna i transnacionalna priroda zločina doprinose da je krajnje teško ubediti tužioca da se prihvati slučaja, jednako kao i dokazati ga na sudu. Izvan Sjedinjenih Država, osude u ovoj novoj oblasti zakona imaju tendenciju da budu blaže nego za konvencionalne zločine, što znači da su policijske snage primorane da ulažu velike resurse, a sve za prilično oskudne rezultate. Međutim, problem s nekim kao što je Dron jeste u tome da bi, što je uspešniji postajao, njegov proizvodni učinak sve više cedio lokalnu i globalnu privredu. Potencijalni gubici zbog veštog mahera kao što

je Dron bili su ogromni. Kako god bilo, u etru se nalaze desetine hiljada aktivnih sajber kriminalaca, a samo će vrlo malo njih ikada biti uhvaćeno.

Premda povučen i neškolovan, Jele je očigledno bio talentovan. Njegova kombinacija preduzetničkog i tehničkog umeća pomoći će mu, po svoj prilici, da se dočeka na noge nakon što preturi preko glave suđenje i odsluži kaznu. Svoje znanje je već bio preneo drugim članovima DarkMarketa, od kojih je jedan već gradio veliku fabriku skimera na drugom kraju sveta. To, međutim, na kraju krajeva, nije bila odgovornost Drona niti detektiva Frizela – brzina kojom se znanje prenosi kroz mračnu stranu Mreže još je jedan ubedljivi razlog da nacionalne policijske snage poboljšaju komunikaciju sa kolegama u inostranstvu.

Posle hapšenja Drona i Matriksa, policija je morala brzo da krene na sledeće mete, pre no što DarkMarketari primete da su njihovi redovni kontakti naglo i umnogome neobjašnjivo nestali s interneta. Tajna služba je, što se toga tiče, bila u boljem položaju, budući da je ChaO, sa svojim ovlašćenjima administratora, već isključio Drona sa foruma.

Dok je Dron još učestvovao na forumu, ChaO je iskoristio svoj autoritet da pokupi tajne zanata mladog tehničara. Čim su on i njegov tim (imao je nekoliko saučesnika) ovladali znanjem, uskratio je Dronu članstvo, baš kao je u decembru 2006. uradio sa JiLsijem. Dron više nije mogao da se oglašava na DarkMarketu, a pošto je većina drugih foruma bila likvidirana u bespoštednoj borbi između DM-a i CardersMarketa, marketinška strategija mladog Kanađanina našla se pred ozbiljnim preprekama. Sklonivši Drona s puta, ChaO je bio zauzet uspostavljanjem sopstvenog takoreći monopola u prodaji skiming uređaja.

Pošto je Dron bio banovan sa DarkMarketa, njegova tri partnera iz Francuske – Theeeel iz okoline Pariza, i Lord Kaisersose i Kalouche u Marseju – nisu ni mogli primetiti da ga je Spenser Frizel uklonio iz opticaja. Bez obzira na to, Tajna služba nije znala kada će nemačka policija, uz podršku FBI-ja, uhapsiti Matrixa, najproduktivnijeg administratora DarkMarketa. A njegov iznenadni nestanak sa foruma će, po svoj prilici, isprepadati preostale članove DM-a.

U Švedskoj, Recka je odmah znao da su snage reda i zakona u pohodu. On i Matrix su dotad svakodnevno razmenjivali prijateljske poruke, pa nije „pao" na čudni post koji se početkom juna

pojavio pod Matrixovim imenom. Majka mi je doživela ozbiljnu nesreću, objašnjavao je Matrix, pa ću neko vreme odsustvovati. Svaki iskusni sajber lopov je smesta zaključio kako je policija preuzela njegov nadimak (što je bilo tačno) i da je to samo „finta".

Lord Kaisersose, Theeeel i društvo su, dabome, bili drugačiji – bili su Francuzi. Francuska je na osobeni način doprinosila sajber kriminalu. Francuski kriminalci su, naime, isto tako bandoglavo frankofoni kao i ostali njihovi zemljaci. Policajac francuskog jezika, Francuska akademija, devedesetih je s nelagodom uočila eksponencijalni porast koji je doživljavao engleski jezik kao globalna *lingua franca*. Međutim, na svoje zadovoljstvo, primećivala je i da je, u digitalnom svetu, većina francuskih hakera i gikova privržena borbi protiv engleskog, tog primarnog izvora jezičkih nečistota.

To je sa sobom nosilo dva značenja: u početku je sajber kriminal u Francuskoj bio istinski nacionalan – nije prelazio granice kao drugde u svetu. Ta zemlja je, inače, predupredila internet tako što je 1982. predstavila svoju vrlo efikasnu informacionu tehnologiju zvanu Minitel, koja je putem linija fiksne telefonije prenosila tekst na video ekran. Posledica toga bila je da su Francuzi posedovali mnogo naprednije razumevanje informacione tehnologije u odnosu na najveći deo ostatka sveta. Sistem Minitela, putem kojeg su klijenti mogli da pretražuju telefonski imenik, proveravaju svoj bankovni račun, šalju cveće ili vode golicave razgovore koristeći *messageries roses* („ružičaste poruke"), bio je znatno bolje obezbeđen protiv hakera nego internet, što delom objašnjava zašto Mreža u Francuskoj tek sada počinje da zasenjuje Minitel.[34] Francuzi su zato bili manje podložni prvim virusnim infekcijama na internetu. Pre svega, relativno malo francuskih hakera je provodilo vreme na forumima poput CarderPlaneta, Shadowcrewa i DarkMarketa.

Takođe, spam imejl je u Francuskoj sporo napredovao. Profit je bio mnogo manje primamljiv od onih koje je generisalo masovno spamovanje na engleskom, španskom i, u poslednje vreme, kineskom govornom području. Naprosto je tržište bilo premalo. Pri tom se, sve donedavno, osamdesetak agenata OCLCTIC-a nije ni trudilo da prati sajber pretnje koje su poticale iz drugih zemalja (za razliku od francuske vojske i obaveštajne službe, koje poseduju

34 Tridesetog juna 2012 (nekoliko meseci posle objavljivanja ove knjige u Americi) francuski Telecom je ugasio Minitel. (Prim. prev.)

izuzetno napredne sajber sposobnosti). Operacija Lord Kaisersose (marsejski tim) i Operacija čvrsti disk (Dron i Theeeel) doprinele su donekle da agenti OCLCTIC-a lakše objasne svojim političkim gospodarima zašto francuka policija mora delotvornije sarađivati s međunarodnim kriminalističkim službama. Možda najviše od svega zapanjuje to što hapšenja koja je izvršio OCLCTIC – koji je sa desetinama naoružanih policajaca upao na adrese u Marseju i u okolini Pariza – uopšte nisu pomenuta u francuskoj štampi: nije bilo nijednog jedinog izveštaja.

Prilikom hapšenja Theeeela, policija se blago šokirala shvativši da mu je tek osamnaest godina – bio je najmlađi uhapšeni DarkMarketar u celom svetu. U karding se uvalio kako bi mogao da plaća školarinu na fakultetu. Ako neke devojke zaključe kako studije finansijski mogu da izguraju samo povremenom prodajom svog tela, sasvim je predvidljivo da i mladi gikovi moraju biti u iskušenju da dopune svoj prihod. A kao što je otkrio Theeeel, kad novac počne da pritiče potocima, te navike teško se odreći.

Francuska policija je u prvo vreme verovala da Lord Kaisersose pripada jednoj od brojnih bandi sitnih kriminalaca koje nastanjuju Marsej, tu francusku Odesu: to je takođe luka u stalnom porastu, s jedinstvenom kulturom (a u slučaju Marseja i sa fenomenalnom kuhinjom). Prateći osumnjičene, policajci su saznali da jedan od saučesnika Kaisersosea, Dustin, poseduje restoran udaljen sat vožnje od grada, te da već ima policijski dosije zbog više sitnih prevara.

Međutim, kad su agenti OCLCTIC-a zajedno s pripadnicima marsejske policije upali u stan osumnjičenog Hakima B. u centru Marseja, shvatili su da Lord Kaisersose pripada višoj klasi. Pored najraznovrsnije kompjuterske opreme, stan je bio ukusno i elegantno nameštен. Hakim nije bio nikakav ulični razbojnik. Bio je talentovani haker čiji je brat, Ali B., slučajno radio u DHL-u. Za sajber kriminalce, malo je firmi koje su tako dragocene kao međunarodne kurirske službe. Sa Alijem kao insajderom u DHL-u, Hakim je bez imalo teškoća mogao da otprema iz Marseja robu i novac a da to niko ne primeti. A to je bilo važno – zato što je Hakim bio jedan od najvećih preprodavaca dampova ukrajinskog kralja kardinga, Maksika.

Za nešto duže od dve godine, Maksik je Hakimu prodao podatke sa 28.000 kreditnih kartica, koje su „unovčene" vredele oko 10 miliona dolara. Uz pomoć svog tima – Alija, Dustina i još jednog

ili dva čoveka – Hakim je slao kartice do bankomata širom južne Francuske. Brižljivo je vodio računa da nikad ne koristi nikakve francuske kartice već samo američke. Da se Tajna služba SAD nije obratila OCLCTIC-u u vezi s ovim slučajem, Lord Kaisersose bio bi i dan-danas slobodan – i mnogo bogatiji.

25.
Nevidljivi čovek

Renukant je verovao da može započeti novi život. Isključenje sa DarkMarketa podstaklo je depresiju koja je potrajala tri nedelje. Sajt koji je stvorio ni iz čega bio je jedino što mu je išta značilo, a to su mu uzeli. Dok je zima 2006. uzmicala pred prolećem 2007, a njegov prvobitni šok izbledeo, lagano ga je obuzeo čudan osećaj oslobođenosti. Ustanovio je da je kadar da se skine s kreka i pića. Magla u njegovom mozgu polako se razilazila i počeo je da ide u teretanu, ne bi li se rešio dela suvišne težine koja se nagomilala za vreme koje je proveo kao opsesivni administrator DarkMarketa. JiLsi je bio omalen i nije mu trebalo dugo da od momka mršavog kao grana postane debeo kao bumbar.

Posle nekoliko nedelja, poslao je administratorima DarkMarketa zahtev da mu dozvole povratak na sajt. Dozvolili su mu, mada su odbili njegovu molbu da se vrati kao administrator. Umesto toga, dodelili su mu jedinstvenu – mada beznačajnu – počasnu titulu „poštovanog člana".

Više nije mogao da ima vlast nad životom i smrću članova sajta, ali je nastavio da pomaže u njegovom glatkom funkcionisanju. Jedan član je osmislio prevaru s kreditnim karticama na benzinskoj pumpi Teksako u Portsmutu, na južnoj obali Engleske. Neko je instalirao mini-kameru u tavanici iznad uređaja za provlačenje kartica na kasi. Ne samo da su kartice bile skimovane nego su i njihovi vlasnici snimani kako unose PIN. Na svoju nesreću, JiLsi je pristao da učini uslugu drugom članu i da posreduje kao garant. Ali i gore od toga, zamolio je trećeg, sa nadimkom Sockaddr, da unovči kartice u Sjedinjenim Državama. Sockaddr je bio glavna krtica Tajne službe na DarkMarketu.

Međutim, učestalost JiLsijeve aktivnosti na forumu se smanjila – njegovi karderski dani su se primicali kraju. Mada još nije smislio šta će posle toga, bio je prilično siguran da je došlo vreme da počne da živi poštenim životom. Morao je da se izvuče iz haosa u kom se nalazio.

Renuovo šesto čulo govorilo mu je i da se događa nešto čudno. Osmatrao je, osluškivao i njušio i na najmanji šum, poput jelena koji oseća opasnost. Učinilo mu se da je primetio dve životinje koje ga progone. Postao je ubeđen kako krajičkom oka vidi čopor lavova oko kafea Java bin. Isto tako, stalno je gledao u nebo očekujući da vidi kako njime kruže lešinari.

Je li to bila paranoja ili su njegova dva života, kao Renua i kao JiLsija, bila u opasnosti da se sudare? U svakom slučaju, bilo je najbolje napraviti plan za sve moguće ishode. Više nije mogao da bezbrižno zanemaruje očigledne znake: kola predugo parkirana blizu kafea; neznance koji su navraćali u njega a naprosto se nisu uklapali – pogrešna demografija, pogrešna odeća. Posle dve ili tri nedelje, Renu je počeo da menja maršrutu kojom je dolazio u Java bin i odlazio iz njega. Naravno, imao je pratnju. Lavove.

Lešinari su bili članovi manje organizovanog ali podjednako pretećeg tima koji su slali upozorenja u vezi s određenim finansijskim obavezama koje je Renu natovario sebi na vrat posle katastrofalne epizode s USB memorijom od pre više od godinu dana. Sad su tražili svoju funtu mesa. Da li bi ijedna od tih grupa bila voljna da pregovara? Ili će morati da im obema pobegne?

Nekoliko meseci pre toga, u martu, JiLsijev slučaj preuzeo je agent Mik Džejmison. Njegova agencija, SOCA, pratila je JiLsija već duže od pola godine, posle dojave od Kita Mularskog. I Tajna služba SAD i FBI su ga već dugo imali na nišanu, zahvaljujući njegovom hiperaktivnom postovanju na takoreći svim kriminalnim sajtovima koji postoje (gotovo u toj meri da se, ako JiLsi nije na vašem sajtu, zapitate je li s vama sve u redu). Njegov izrazito vedri, dobrodušni avatar, pirat s povezom na oku i trorogim šeširom, bio je neukrotiv.

SOCA je bila jedina agencija koja je znala za DarkMarket operacije pod vođstvom Tajne službe i FBI-ja i, u izvesnom stepenu, ta britanska služba za borbu protiv organizovanog kriminala delovala je kao pasivni mirotvorac, uspevši makar da obezbedi da datum hapšenja Lorda Kaisersosea i Theeeela u Francuskoj bude isti onaj koji je planiran za Matrixa u Nemačkoj i JiLsija u Engleskoj.

Tim za praćenje je još od februara držao foto-aparate i prislušne uređaje usmerene na Java bin. Agenti nisu ispuštali Renua iz vida. Zapisivali su satnicu njegovih susreta s nekim ljudima,

kad je često govorio na tamilskom. Videli su ga kako predaje gotovinu i USB memoriju ljudima koji bi na trenutak zaustavili kola pored njega i potom odjurili dalje. Čak su natrapali na još jednog člana DarkMarketa koji je takođe zalazio u Java bin. Međutim, hteli su Renua. Pomoću telefoto sočiva fotografisali su monitor njegovog kompjutera. Jedan Džejmisonov kolega se infiltrirao na DarkMarket kao obični član, tako da su mogli da prate veliki deo JiLsijevih postova. Pored toga, Mularski im je doturao neprocenjivo vredne obaveštajne podatke. Međutim, još nisu posedovali neosporan dokaz da je Renukant Subramanijam JiLsi. Za to će morati da ga uhapse.

Razne policijske snage rešile su da krenu na njega u drugoj nedelji juna. Tajna služba i FBI su konačno postigli kakav-takav sporazum – dan D je bio 12. jun. Potom su taj plan upropastili anonimni mejlovi koje je dobio Matrix001. Ako JiLsijevo hapšenje propadne, postojali su dobri izgledi da se to u roku od nekoliko minuta pročuje preko DarkMarketa, i višegodišnje mukotrpne pripreme bile bi uzaludne.

A onda su se Džejmisonovi najcrnji strahovi obistinili – dva ili tri dana posle Matrixovog hapšenja, JiLsi je prosto ispario. Jednog jutra nije otišao u Java bin već do obližnjeg stadiona Vembli, uputivši se u centar Londona. Dok je prolazio pored robne kuće IKEA na Nord cirkularu, londonskoj vazda zakrčenoj unutrašnjoj obilaznici, primetio je muškarca osobenog izgleda. Ili je to bila žena? Nije bio siguran. Osoba se možda najbolje mogla opisati kao androgina. Nastavio je dalje prema Vembli parku. Kad se uputio ka pešačkom prolazu pored stanice metroa, spazio je gore na mostu dugokosog muškarca koji ga je posmatrao i razgovarao telefonom.

Nakon što se na liniji Džubili ukrcao u voz do centra, JiLsi je na stanici Grin park preseo u voz prema Pikadiliju, da bi potom sišao na Lester skveru; međutim, kao što se na toj stanici mnogima desi, izašao je na pogrešnom izlazu i morao da se vraća do trga.

Srce mu je stalo: tamo je stajao gospodin Androgini. A idući prema Lester skveru, prepunom turista i uličnih umetnika, Renu je umalo naleteo na gospodina Dugokosog. Sad više nije bilo sumnje – pratili su svaki njegov korak.

Utrčao je u kineski restoran i seo da ruča i razmotri mogućnosti. Izašao je na sunce i potom skrenuo u Sent Martin, uličicu

pored Nacionalne galerije koja se sužava u pasaž i potom izbija na Trafalgar skver.

Rojeći se oko Nelsonovog stuba, posetioci su se divili prekrasnoj, četiri metra visokoj statui koja je zauzimala Četvrtu plintu, na kojoj se eksponati smenjuju svakih osamnaestak meseci. *Trudna Alison Laper* (*Alison Lapper Pregnant*) predstavlja istoimenu britansku slikarku nagu i u poodmakloj trudnoći. Gospođica Laper je rođena bez ruku, a odluka da se statua postavi na tom mestu izazvala je u to vreme veliku kontroverzu. Privlačila je mnoštvo ljudi i, kad je Renu počeo da se probija kroz plimni talas turista, njegovi pratioci su zaostali. On je pak uskočio u prvi autobus i popeo se na krov. Dok je vozilo skretalo u Ulicu Sent Martin, pogledao je dole i načas ugledao gospodina Androginog i gospodina Dugokosog kako se očajnički osvrću naokolo u potrazi za svojim iščezlim plenom.

Renu je nestao. Ali nije bio jedini – JiLsi je pre toga postavio na internet svoj poslednji post.

Oko dve nedelje kasnije, Renukant se uputio prema jednoj od nekoliko nekretnina koje je, ako ih i nije sve posedovao, svakako iskoristio kao zalog za podizanje kredita. Skoro je bio stigao do kuće, koja je ležala pod samom sletnom putanjom aerodroma Hitrou, kad mu je zazvonio telefon. Drugar koji je stanovao tamo upozoravao ga je da ne dolazi. Policija je upravo upala u kuću mašući nalogom za njegovo hapšenje.

Vođa istrage o JiLsiju, agent SOCA Mik Džejmison, već je bio posetio Renuovo glavno prebivalište u Koniston gardensu, kao i nekoliko drugih. Osim što se kao JiLsi angažovao na DarkMarketu, Šrilankanac je bio i stručnjak za prevare sa hipotekarnim kreditima. Kako bi obebedio zajmove na osnovu raznoraznih nekretnina u severnom, zapadnom i južnom Londonu, nije se libio da masno laže u vezi sa svojim profesionalnim i finansijskim okolnostima. Britanija nije podlegla pomami za hipotekarnim („sabprajm") kreditima koja je zahvatila finansijsku industriju u SAD. Ipak, zloglasni sistem samosertifikovanja, u kom se vaša reč smatra dovoljnim dokazom o visini vaših prihoda, udružen s praksom izdavanja kredita u visini petostruke godišnje plate podnosioca zahteva (u trezvenijim vremenima to nije smelo da premaši tri godišnje plate), značio je da je u UK bilo relativno lako izvesti prevaru s hipotekarnim kreditima. Na tržištu je vladala tako

besomučna konkurencija da je pretvaranje da ništa ne vide postalo najbolja praksa u bankarskoj industriji.

Međutim, posle pomenutog telefonskog poziva, Renuu je bilo više stalo da nekako ispliva iz nevolja u kojima se davio nego da razmišlja o sitnim slovima raznih prevara koje je izveo. Istog časa je odlučio da ode u ilegalu. Tri nedelje je spavao gde je stigao, izbegavao sve adrese za koje je pretpostavljao da su pod nekom vrstom nadzora. Kad je dobio dojavu o upadu policije u njegovu kuću, imao je uza se oko petsto funti.

Život je i pre bio grozničav i rizičan, ali Renu je oduvek pomalo uživao u tome što se pomalo osećao kao junak špijunskih romana: nikad se nije dugo zadržavao na istoj adresi, kradom je predavao USB memoriju kontaktima sumnjivog izgleda i, dabome, veličali su ga kao gospodara karding sajtova a da niko nije znao ko je on. Isprva je mislio kako će noćivanje u kartonskim kutijama pod mostovima, s gomilom pijanaca, doprineti toj enigmatičnoj auri. Međutim, kad je novca ponestalo a on spao takoreći na životarenje od danas do sutra, Renukant Subramanijam – iznuren, prljav i bolestan – zaključio je su ga bežanje i skrivanje saterali u ćorsokak.

Trećeg jula 2007. ušao je u policijsku stanicu Vembli park i predao se. Lakši deo Operacije DarkMarket bio je završen.

Interludij

Zemlja o kojoj ne znam ni šta ni gde

Talin, Estonija

Četiri dana pre zvaničnog datuma održavanja opštih izbora u proleće 2007, mala baltička država Estonija, s populacijom od svega 1,25 miliona, prva na svetu ponudila je svojim građanima mogućnost da daju glas na parlamentarnim izborima a da se pri tom ne pomere od svog PC-ja. Cilj eksperimenta, pod uslovom da uspe, bilo je održavanje potpuno „virtualnih izbora" četiri godine kasnije, 2011.

Da bi Estonija napravila taj značajni skok prema digitalnoj budućnosti, mnogo je kockica moralo da se složi – ne samo da su sistemi morali da funkcionišu, već su morali i da budu obezbeđeni od spoljnih napada. Godinu dana ranije, ta država je zvanično predstavila svoj Tim za vanredne situacije u kompjuterskim sistemima (Computer Emergency Response Team, CERT), čiji je glavni zadatak bio da reaguje na sve upade (slučajne ili zlonamerne) u internet domen sa estonskim sufiksom: .ee. To obuhvata konstantno praćenje protoka internet saobraćaja koji se odvija u zemlji, oko nje i iz nje u potrazi za bilo kakvim nenormalnim obrascima.

Čovek odgovoran za kompjutersku sigurnost cele zemlje je tihi Hilar Arelajd, koji uvek izgleda kao da je maločas ustao iz kreveta, i to nerado. Premda možda deluje rasejano, Arelajd poseduje odlučnost koja ga je uzdigla kroz hijerarhiju estonske policije, u kojoj je počeo kao običan saobraćajac u malom mestu. „Međutim, voleo sam kompjutere, pa sam prvo dobio premeštaj ovde u Talin, da bi me naposletku postavili za glavnog informatičara državne policije." I trebalo je – definitivno izgleda kao gik. I definitivno ne izgleda kao pandur (osim, ako baš mora, kao policajac iz odseka za narkotike osamdesetih godina prošlog veka,

koji se nalazi na tajnom zadatku), pa je možda i iz modnih razloga, između svega ostalog, 2006. prešao da vodi CERT.

Na dan virtualnih izbora 2007, CERT i Hilarove bivše kolege iz kriminalističke službe bili su u pripravnosti. „Naravno", objasnio je, „primetili smo da je neko pokrenuo botsken na izbornom sistemu." Kako izgleda, neko je poslao automatsku sondu s nalogom da na izbornim serverima potraži sve portove koji su nekom greškom možda ostali otvoreni. „To nije bilo naročito ozbiljno, pošto se botskenovi vrlo lako detektuju", nastavio je Hilar, „ali je ipak predstavljalo stvarnu bezbednosnu pretnju."

Zatim je, nadimajući se od ponosa – onoliko koliko je opušten tip poput Hilara to u stanju – izjavio: „Petnaest minuta nakon što smo primetili botsken, policajac je pokucao na vrata na adresi u Rapli, pedeset kilometara južno od Talina, i upitao stanara: 'Zašto ste pustili botsken na izbornim kompjuterima?'"

U svetu sajber bezbednosti, petnaest minuta od detekcije upada u sistem pa do policajca koji dolazi na lokaciju kompjutera iz kog je upad potekao više je nego impresivno – briljantno je. „Srećom po nas pa smo tada odradili dobar posao", rekao je Hilar, „zato što smo posle toga bili potpuno spremni za napad koji je došao potkraj aprila."

Taj „veliki napad", dva meseca posle izbora, bio je još nešto po čemu je Estonija bila „prva" otkako postoji virtualni prostor; naime, kako je bila izložena neprekidnim napadima na svoje mreže, to ju je naposletku nateralo da zatvori internet veze sa spoljnim svetom. Neki smatraju da je bio prvi zabeleženi slučaj sajber ratovanja.

Hilara sam potražio mesec dana posle moje posete Googleu u Silicijumskoj dolini. Putovanje na istok dovelo me je u Talin, pitoresknu prestonicu te najsevernije baltičke države. Zidine starog grada skrivaju raskošnu mešavinu skandinavskih, nemačkih i slovenskih arhitektonskih stilova, po kojima se vidi kako su nekadašnje imperijalne težnje suseda Estonije na severu, istoku i zapadu tek pre malo više od dvadeset godina konačno ustuknule pred estonskom primarnom, domaćom kulturom (premda gotovo četvrtinu stanovništva još uvek čine Rusi).

Vrata do vrata s pravoslavnim, luteranskim i katoličkim crkvama nalaze se kao bajagi rustični restorani namenjeni turistima i, posle obilatog obroka, živahni noćni klubovi u kojima ćete igrankom zaokružiti večernji provod. Kao mesto održavanja

momačke večeri, Estonija među pijanim mladim Englezima još nije popularna kao susedna Letonija, ali ipak ima svoju bednu stranu. Među klubovima se nalazi i uzbudljivi Depeche Mode Baar (Bar Depeš mod), u kom puštaju samo ploče istoimene grupe iz Eseksa, iz 1980-ih, a dekorisan je kao hram kulturnom nasleđu Britanije iz prvih dana vladavine Margaret Tačer.

Talinova čudna ali gostoljubiva atmosfera bila je još izrazitija zbog toga što sam stigao samo nedelju dana pre Ivanjdana i svitanja legendarnih Belih noći. Mrak pada tek posle ponoći, a već sat i po kasnije počne da sviće. Već za sedam dana, obdanica će trajati dvadeset četiri sata.

Ova zbrkana raskrsnica imperijalnih težnji, osobenih kulturnih ikona savremenog doba i sanjive prirode svetla obrazuje idealnu pozadinu za godišnji skup Kooperativnog centra za sajber odbranu i nadmoć (Cooperative Cyber Defence Centre of Excellence, CCDOE), koji, uz finansijsku podršku NATO-a, istražuje sve aspekte sajber ratovanja. Likovi na tom skupu žive u privremenoj Zemlji čuda, u kojoj se konvencije često zanemaruju – konjski repovi i naočari sa žičanim okvirom ozbiljno razmenjuju informacije s uštirkanim vojničkim uniformama u vezi sa „slabim tačkama SQL ubacivanja". Državni službenici u odelima i kravatama zadubljeni su u razgovor s mladićima u farmerkama i majicama, i razglabaju o pokvarenosti „napada preko čoveka u sredini" („man-in-the-middle attack", odn. prisluškivanje preusmeravanjem saobraćaja preko napadačeve radne stanice).

Da bi shvatio makar i puke osnove sajber bezbednosti u njenoj svekolikoj raznolikosti, čovek mora biti spreman da nauči bezbroj novih idioma koji se stalno dodaju ili menjaju. U suprotnom, može vam se desiti da slušate razgovor koji je, što se tiče osnovnog vokabulara i sintakse, sasvim sigurno engleski, ali, bez obzira na to, zvuči potpuno besmisleno onima koji nisu podučeni tom tajanstvenom jeziku. Neprijatno vam je, dabome, kad morate stalno da zapitkujete ljude koji ga tečno govore zašto „preopterećenje bafera" može imati uznemirujuće posledice po bezbednost vaše mreže, ali gikovi nisu snishodljiva ekipa i generalno će vam rado izaći u susret i objasniti.

Estonija možda jeste mala, ali je elektronski najpovezanija zemlja Evrope i jedna od vodećih digitalnih sila na svetu, iz koje je – između ostalog – došao Skype. Na većini mesta imate besplatnu bežičnu konekciju, budući da se konektivnost smatra

osnovnim pravom a ne povlasticom. Tamo nećete naći hotele koji vam uzimaju novac u zamenu za pristup internetu.

Međutim, sa Hilarom Arelajdom nisam razgovarao o naprednom pristupu Estonije, već o njenom legendardnom položaju u sada sve obimnijoj istoriji međunarodnih digitalnih sukoba.

Početkom 2007. estonska vlada je obznanila svoju nameru da premesti spomenik Crvenoarmejcima palim u Velikom patriotskom ratu (kako Rusi nazivaju Drugi svetski rat) iz srca Talina na glavno gradsko groblje koje se, istini za volju, nalazi nedaleko od centra grada. Rusija i njeno rukovodstvo doživeli su to kao smrtnu uvredu, pa čak i kao dokaz uskrsnuća fašističkog nacionalizma Estonaca (svih 750 hiljada koliko ih ima) i ponižavanje onih vojnika Crvene armije koji su žrtvovali život oslobađajući Estoniju od nacističkog jarma.

Spor oko bronzanog vojnika je eskalirao. Ruski mediji, što u Estoniji, što s druge strane granice, u Rusiji, podstakli su istinsku zabrinutost estonske ruske manjine i uskoro je napetost dosegla vrhunac. Dvadeset sedmog aprila posle podne, u centru Talina okupile su se stotine mladih etničkih Rusa, građana Estonije. Protest protiv uklanjanja spomenika bio je miroljubiv i dobrodušan, sve dok jedna grupa nije pokušala da probije policijski kordon koji je štitio statuu. Izbio je siloviti okršaj, koji se brzo raširio – do večeri je stari grad, inače pod zaštitom Uneska, bleštao osvetljen zapaljenim automobilima, izlozi su bili porazbijani a njihov sadržaj opljačkan.

Dok su neredi pretili da se raširе još više, Moskva je izdavala upozorenja u kojima je opisivala brutalnost estonske policije, a zemlja koja je manje od dve decenije pre toga stekla nezavisnost od Sovjetskog Saveza, našla se u kandžama neizvesnosti i straha. Bilo je krajnje neverovatno da će Rusija ponuditi Estoniji „bratsku pomoć", da upotrebim sovjetski eufemizam za slanje tenkova. Najzad, Estonija je sada bila članica NATO-a i bilo je nezamislivo da bi Rusija poželela da pokrene NATO-ov mehanizam zajamčene odbrane teritorije – svi za jednog i jedan za sve – zbog tamo neke proklete statue!

Srećom po sve nas, Kremlj uistinu nije pokazao nikakvu nameru da pruži bilo kakav vid bratske pomoći, ali dok je u centru Talina sve praštalo i šištalo od učesnika u neredima i onih što su palili zastave, hakeri su otvarali novi front u ovom osobenom konfliktu.

Te večeri, sajtovi estonskog predsednika i nekoliko državnih ministarstava počeli su da primaju neobično velike količine spam imejlova, dok je fotografija premijera na sajtu njegove stranke bila zamrljana. Sobe za ćaskanje na ruskom jeziku počele su da nagovaraju hakere da pokreću napade na estonske sajtove i distribuirale su softver potreban za to. Prema izvorima navedenim u depeši Ambasade SAD Vašingtonu (obelodanjenim posredstvom Wikileaksa), početni napadi bili su tehnički nesofisticirani i „više su ličili na sajber nerede nego na sajber rat".

Za vreme vikenda, međutim, napadi su od poplave spamova prerasli u DDoS napade. Hakeri su stvorili na desetine onih vraških botnetova, koji su zarazili kompjutere širom sveta i primorali ih da traže pristup estonskim sajtovima. Bili su to moćni napadi – predsednički sajt, „koji normalno ima kapacitet od dva miliona megabita u sekundi, bio je preplavljen saobraćajem od skoro 200 miliona Mbit/s", prema navodima depeše upućene iz ambasade. S tim se još i moglo izaći na kraj, ali 3. maja „sajber napadi su se sa sajtova i servera vlade Estonije proširili na privatne sajtove".

Te večeri, negde oko deset sati, u domu Jana Prisalua na periferiji Talina zazvonio je telefon. „Iz firme su mi javili da nam kanali redom padaju", priseća se on. Kao šef IT bezbednosti u najvećoj estonskoj banci Hansabank, Prisalu se izbezumio. „Potom sam dobio SMS, koji me je obavestio da je oboren i naš servis za internet banking."

Svi su bili u stanju opšte uzbune: desetine hiljada kompjutera zatrpavalo je sisteme Hansabanka zahtevima za informacije. Prisalu se smesta bacio u grozničavu elektronsku akciju i ubrzo otkrio da se Hansabank nalazi pod napadom botneta koji obuhvata oko 80.000 kompjutera. Prateći napade do mesta nastanka, ustanovio je da dolaze sa servera u Maleziji. To, doduše, nije ništa dokazivalo, budući da su napadači uspešno zamaskirali putanju koja je vodila dalje od Malezije. Međutim, odmah mu je bilo jasno da ima posla s ozbiljnim napadom. „Bio je vrlo snažan", rekao je. Botnet od 80.000 kompjutera je ogromno čudovište kadro da za svega nekoliko minuta potpuno paralište celokupni sistem kompanije.

Zahvaljujući Prisaluovim merama predostrožnosti, Hansabank je bila dobro pripremljena i imala je moćne servere. Bili su to alternativni sajtovi s prekopiranim sadržajem (što je otežavalo

uspeh DDoS napada). Međutim, iako je sajt Hansabanka ostao onlajn, glavni izvor Ambasade SAD izvestio je da je čitava rabota koštala banku „najmanje 10 miliona evra".

Sledeće mete bili su estonski mediji, uključujući i dnevne novine, čiji je sajt sa vestima bio ubedljivo najčešće posećen. „Zamislite, ako možete, psihološki efekat", rekao je jedan posmatrač, „kad Estonac pokušava da plati svoje račune ali ne može, ili kad pokušava da pročita vesti na internetu ali ne može." Vlada je bila u stanju najviše pripravnosti, duboko zabrinuta da sve jači napadi predstavljaju „zastrašujuću pretnju ključnoj privrednoj i društvenoj infrastrukturi".

Dotad su već Hilar Arelajd i njegov tim bili u potpunosti mobilisani. Estonijski CERT je reagovao tako što su uz pomoć prijatelja u inostranstvu, pre svega u Finskoj i Švedskoj, proširili širokopojasni internet (broadband) tako što su obrazovali „cevovod" („pipeline") za dotok signala u zemlju. „Očekivali smo da će se možda desiti nešto ovakvo i zato smo bili u pripravnosti", sećao se Hilar. „U tome se sastojala greška Rusa. Ako hoćeš da uspešno izvedeš jedan ovakav napad, moraš veoma dobro da poznaješ neprijatelja i moraš biti blizak s njim", rekao je objašnjavajući da Rusi nisu predvideli visok nivo pripremljenosti Estonije. „Da su dobro razmislili o tome", nastavio je on, „znali bi da su naši sistemi, zbog nedavnih izbora, u stanju visoke pripravnosti."

Zahvaljujući koordinaciji vlade, policije, banaka i CERT-a, posledice napada po obične građane zadržane su u razumnim granicama. Hansabank je sačuvala svoj internet banking, ali druge dve velike banke nisu uspele. Umesto toga, ljudi su se prosto prebacili na njihove filijale. Mobilna telefonija je bila ometana i, nakon što je vlada naredila zatvaranje veza Estonije sa spoljnim svetom, komunikacija s tom zemljom bila je nekoliko dana veoma otežana. Suprotno početnim izveštajima, semafori u Talinu nisu prestali da rade, ali rad vlade i medija se povremeno prekidao.

Napadi, čiji je intenzitet varirao, potrajali su dve nedelje, kulminirajući masivnim napadom 9. maja, na dan pobede Crvene armije nad nacistima u Evropi. Tada je estonska vlada, iznurena nemilosrdnom poplavom DDoS napada, odlučila da odseče internet sistem svoje zemlje od ostatka sveta. DDoS napadi sveli su se na slabašno curenje, da bi 19. maja sasvim prestali.

Događaji u Estoniji imali su vrlo ozbiljne implikacije. U političkom smislu bilo je savršeno jasno da su napadi potekli iz Rusije, ali vlada u Moskvi je, sasvim predvidljivo, negirala svaku odgovornost za njih. A i sasvim je moguće da nije bilo nikakve zvanične umešanosti. Istraživači nisu uspeli da uđu u trag izvoru napada. Pod pretpostavkom da su zaista došli iz Rusije, međutim, vlada je morala da zna za njih, zbog njihovog sveznajućeg sistema za praćenje, SORM-2. Ipak, u Rusiji se u to vreme odvijalo tako mnogo vanredne internet aktivnosti, da je možda čak i legendarni SORM-2 imao teškoća da drži korak sa svime. Ko zna? Jer, napad na Estoniju je jasno pokazao da, premda možete vrlo razborito pretpostaviti ko podstiče ovakve događaje, nikad ne možete biti sasvim sigurni u to.

Poput svih vlada, i ruska je evoluirala svoj jedinstveni stav prema internetu, njegovoj funkciji i odnosu između države i krajnjeg korisnika. Moskva je rano, još početkom devedesetih, shvatila da je politički i bezbednosni značaj interneta toliki da zavređuje punu pažnju jedne od najdugovečnijih i najuspešnijih institucija u zemlji: tajne policije. Ukratko, FSB (bliski sledbenik KGB-a) razvio je sposobnost da prati svaki paket podataka koji putem interneta uđe u zemlju, koji izađe iz zemlje ili kruži po njoj. Taj sistem poznat je pod primereno zlokobnim imenom SORM-2, doslovno „sistem za operativno-istražne aktivnosti".

SORM-2 je istinski zastrašujući. Zatražite li putem Mreže informaciju sa svog kompjutera u Vladivostoku ili Krasnodaru, kada ona stigne do vašeg ISP-a, tj. provajdera internet usluga, duplikat paketa će poslušno otkaskati do centrale FSB u Moskvi, gde će ga čitati, razbijati glavu nad njim, smejati mu se i (ko zna?) upotrebiti ga kao dokaz protiv vas, ako se FSB-u tako prohte. U najmanju ruku, biće sačuvan u arhivi.

SORM-2 ne zahteva samo da ruski internet provajderi prosleđuju *celokupnu* internet aktivnost u štab FSB-a već, da zlo bude gore, primorava provajdere da kupe neophodnu opremu (koja staje više od 10.000 dolara) i da finansiraju troškove servisa. Ti troškovi se, razume se, prenose na klijente, koji na taj način iz svog džepa plaćaju za moćni instrument ugnjetavanja čije su oni sami glavne žrtve.

Ruska država je tako u položaju da putem mreže zna ko šta radi, kad i kome, a verovatno i zašto. Naravno, lukavi ruski korisnik kompjutera mogao bi skovati plan da zaobiđe sveviđeći SORM-2

tako što će enkriptovati svoje podatke i pretragu interneta. Međutim, prisetite se – enkripcija je u Rusiji nezakonita i jedan jedini digitalno zaključani fajl bio bi dovoljan da vam kupi kartu za Sibir u jednom pravcu.

Sve to uopšte ne znači da internet režimi vlada na Zapadu predstavljaju uzoran primer slobode govora. Naprotiv, kako naša zavisnost od interneta postaje jača, tako se pojačava i želja, sposobnost i spremnost državnih vlada da je kontrolišu. Uprkos uobičajenim protestima javnih zvaničnika i političara kako nikakav sličan proces nije u toku, mučno i sporo umiranje internet privatnosti na Zapadu, pogotovo u Ujedinjenom Kraljevstvu i Sjedinjenim Državama, predstavlja tužnu – premda vidljivu – stvarnost i po svoj prilici je neizbežno.

Ta reakcija na 11. septembar, u ime borbe protiv terorizma, ozbiljno je umanjila našu slobodu od uplitanja države u Mrežu. Glavni instrument za to je u SAD bio program Totalne informacione budnosti (Total Information Awareness, TIA), mada je čak i Bušova administracija, sa svojim urođenim nedostatkom sluha, naposletku shvatila da taj naziv podstiče toliko orvelovskih asocijacija da bi ga trebalo promeniti; tako je preimenovan u Terrorism Information Awareness (takođe TIA).[35]

TIA je omogućavala da DARPA (Defense Advanced Research Projects Agency – Agencija za napredne istraživačke projekte namenjene odbrani), krilu Pentagona zaduženom za istraživanja i pretrage, ima znatan pristup podacima dobijenim iz privatnih komunikacija. Mada je program naposletku zatvoren, vlada je zadržala mnoga njegova ovlašćenja i podelila ih raznim agencijama u Sjedinjenim Državama.

U slučaju koji je označio prekretnicu u sudstvu, doneta je odluka bez presedana kad je Vrhovni sud dozvolio da FBI upotrebi kiloger trojance na kompjuterima osumnjičenih, premda isključivo pod nadzorom suda. To je omogućilo FBI-ju da beleži sve što osumnjičeni radi na svom kompjuteru, što je isto što radi sajber kriminalac kada kilogerom zarazi kompjuter trećeg lica. Na smeni milenijuma, Evropski parlament je potvrdio postojanje programa Echelon, globalnog špijunskog programa Sjedinjenih Država, koji je navodno sposoban da se usredsredi na digitalne komunikacije bilo gde u svetu.

35 Otprilike: „Budnost nad terorističkim informacijama". (Prim. prev.)

Prema direktivi izdatoj za vreme predsedavanja Velike Britanije Evropskoj uniji, internet provajderi u Evropi imaju obavezu da od šest meseci do dve godine čuvaju sav kompjuterski saobraćaj (ovo važi i za mobilne telefone) – podatke kojima, u skladu sa zakonima svoje države, mogu da pristupe najrazličitije vladine agencije. Ukoliko se ovi potezi koji vode ka digitalnom nadzoru nastave, zapadne vlade (obično u ime antiterorističkih strategija i kriminalističkih službi) biće u još boljem položaju da prate kretanje i navike svojih građana.

Naš odabrani put najbolje su opisali istraživači Londonskog ekonomskog fakulteta (London School of Economics). U junu 2009. zamolili su čitaoca da zamisli:

> vladu koja ima gluvog bezbednjaka koji prati svaku pojedinu osobu gde god da se ona kreće. Agent ne čuje sadržaj interakcija, ali zato posmatra svaki najmanji detalj nečijeg života: kad se ta osoba budi, kako odlazi na posao, s kim i koliko dugo razgovara, poslovanje njene firme, njeno zdravstveno stanje, ljude s kojima se susreće na ulici, njene društvene aktivnosti, političku pripadnost, novine i članke koje u njima čita i njenu reakciju na njih, namirnice u njenoj korpi u samousluzi, da li se zdravo hrani, ima li dobar brak, njene vanbračne afere, osobu s kojom se zabavlja ako nije u braku i intimne odnose. Budući da se većina ovih interakcija danas na određenom nivou odvija posredstvom telekomunikacionih usluga ili putem mobilnih uređaja, sve ove informacije će sada boraviti kod naših internet provajdera, spremne, čekajući da im vlada pristupi.

Mi na Zapadu makar imamo kakvu-takvu šansu da se borimo i odupremo nekim više drakonskim ovlašćenjima koje raznorazni ogranci vlasti teže da steknu nad internet aktivnostima građana.

S obzirom na snagu pokreta za građanska prava na Zapadu i sveobuhvatni nadzor KGB-a nad internetom, čovek bi pomislio da će Rusija za sajber kriminalce predstavljati neumoljivo neprijateljsko okruženje. A ipak, Ruska Federacija postala je jedan od velikih centara globalnog sajber kriminala. Stopa policijskih akcija je dostojna žaljenja, dok je broj osuđenih jedva dvocifren. Razlog je svima više nego jasan, iako ga niko ne govori naglas. Pod uslovom da su njihovi napadi locirani u Zapadnoj Evropi i

Sjedinjenim Državama, ruski sajber kriminalci mogu do mile volje da kloniraju koliko god hoće kreditnih kartica, i da hakuju onoliko bankovnih računa i distribuiraju onoliko spamova koliko im se prohte. Ruski haker koji počne da pljačka Ruse bio bi strpan na zadnje sedište neobeleženog vozila dok si rekao KGB.

U zamenu za to, dabome, zatrebaju li ruskoj vladi nekim slučajem usluge hakera koji će lansirati obogaljujuće sajber napade na onoga ko se smatra neprijateljem, za hakera je po svoj prilici najbolje da sarađuje.

Dve hiljade sedma bila je pobedonosno razdoblje za labavu organizaciju kompanija sa sedištem u Sankt Peterburgu, poznatu kao Ruska poslovna mreža (Russian Business Network, RBN). Ovaj tajanstveni akronim nudio je pojedincima i kompanijama sajt hosting – bio je poznat kao kralj neprobojnih hostera. Kompanije koje nude tu vrstu usluga u suštini daju svojim klijentima do znanja da nisu zainteresovane za sadržaj ili funkciju sajta i da će se, u zamenu za mnogo veću naknadu, odupreti svim legalnim ili digitalnim pokušajima obaranja tih sajtova.

Nije sav neprobojni hosting predviđen da bude način za zaobilaženje zakona, ali kriminalci i pirati često koriste takve usluge. Pojedincima i grupama umešanim u distribuciju dečje pornografije, na primer, one su takoreći neophodne i poznato je da se u poslovnim knjigama RBN-a nalaze i takvi klijenti, kao što je ustanovilo više istraživačkih odseka bezbednosnih kompanija.

Spamhaus, tajna antispam operacija u Kardifu, zabeležila je da je Ruska poslovna mreža 2006. i 2007, dok joj je posao cvetao, kontrolisala 2.048 internet adresa. Svrstala je RBN među „najgore spamere na svetu" i utočište ogromnom broju „mreža povezanih sa dečjom pornografijom, malverom, fišingom i hostingom sajber kriminala".

Primarni značaj RBN-a leži u profitabilnosti takvih organizacija za neprobojni hosting, koje naplaćuju mesečnu naknadu od 600 ili više dolara. Za legitimne sajtove, mesečna naknada iznosi svega desetinu te sume.

Međutim, mnogo zanimljivija je njena druga uloga. Napadi na Estoniju počeli su milionima spam imejlova koji su se obrušili na kompjuterske mreže estonske vlade. Kasnije je Fransoa Paže, koji radi za McAffee, američkog giganta u oblasti kompjuterske bezbednosti, analizirao sadržaj spamova i ustanovio da su identični standardnim imejlovima RBN-a. Štaviše, Endi Old, šef

odseka za obaveštajnu delatnost u sajberspejsu britanske kriminalističke službe SOCA, izvestio je da je britanska policija, u svom kratkotrajnom terenskom posmatranju RBN-a u Sankt Peterburgu, uspela da utvrdi kako RBN uspeva da funkcioniše delom i zato što podmićuje lokalnu policiju i sudije.

Moguće je, ali ipak nije verovatno da je RBN podstakla napade na Estoniju. Verovatnije je da je bila plaćena da ih pokrene ili da su vlasti zatražile od nje da učestvuje u tom patriotskom činu. Ta veza između kompleksa internet provajdera sa sedištem u Sankt Peterburgu, specijalizovanih za kriminalne aktivnosti, i sajber napada na Estoniju, naglašava jednu od najvećih enigmi u samom središtu kompjuterskog kriminala i kompjuterske bezbednosti.

Na internetu postoje tri glavne „pretnje", a svaka se manifestuje u najrazličitijim oblicima. Kao prvo, tu je sajber kriminal. U svom najosnovnijem obliku, sajber kriminal se sastoji od „kardinga", krađe i kloniranja podataka s kreditnih kartica zarad stvaranja finansijske dobiti. Pored kardinga, tu je još tušta i tma drugih prevara. Među najunosnijima je, na primer, takozvani „skerver" („scareware"), koji je usavršila kompanija pod imenom Inovative Marketing, sa sedištem u Ukrajini. IM je u ukrajinskoj prestonici Kijevu zapošljavao desetine mladih ljudi, od kojih je većina verovala da rade za visokotehnološku kompaniju koja prodaje legitimni bezbednosni softver. Samo što to nije bio slučaj.

Kompanija je slala tzv. rog adver (rogue adware) koji, nakon što ga korisnik instalira na svom kompjuteru, inicirala iskakanje pop-ap prozora na pretraživaču, koji je upozoravao korisnika da virus ugrožava njegovu mašinu. Jedini način, objašnjavao je oglas, da oslobodi svoj kompjuter elektronskih buba koje gamižu po njegovom hard disku i RAM memoriji, jeste da klikne na link i kupi „Malware Destroyer 2009" („uništilac malvera"), da navedem samo jedan od njihovih bezbrojnih proizvoda.

Pošto daunloudujete Malware Destroyer (za 40 dolara), IM bi vam naložio da uklonite svoj postojeći antivirus sistem, kao što je Norton, i instalirate njegov proizvod. Kad se instalira, međutim, nije radio baš ništa – bio je to potpuno prazan softver, iako ste vi sada bili, razume se, podložni infekciji od strane svakog virusa s kojim vam se ukrste putevi, pri čemu ste za tu sumnjivu povlasticu još i platili.

Ovu operaciju počeo je da nadzire istraživač za McAffee iz Hamburga, Dirk Kolberg. Pratio je skerver natrag do njegovog izvora u Istočnoj Aziji i ustanovio da je administrator IM-ovih servera ostavio neke portove širom otvorene, pa je Kolberg mogao slobodno da lunja po serveru i razgleda ga. Ono što je otkrio oduzimalo je dah. Innovative Marketing je zarađivao toliko novca da je otvorio tri pozivna centra – po jedan za englesko, nemačko i francusko govorno područje – kako bi pomagao zblanutim kupcima koji su pokušavali da instaliraju njihove neupotrebljive proizvode. Prošetavši kroz potvrde o uplatama, koje je takođe pronašao na serveru, Kolberg je izračunao da je ova skerver prevara generisala desetine miliona dolara prihoda menadžmentu kompanije, u jednom od najteatralnijih primera internet kriminala.

Pored skervera, tu su „pump and dump" šeme, koje obuhvataju hakere koji upadaju na finansijske sajtove i digitalno naduvavaju cene deonica, da bi zatim prodali one u svom vlasništvu, posle čega opet puste da im se cena strmoglavi. Tu su i prevare s platnim listama, kada kriminalci hakuju kompjuter korporacije i u bazu podataka kadrovskog odeljenja dodaju fantomske zaposlene. Međutim, hakeri tim zaposlenima daju stvarne plate; one se svakog meseca isplaćuju takozvanim „mazgama", koje za mali procenat prebacuju taj novac u banku daleko od mesta gde je zločin zapravo počinjen.

Baš kao što Mreža nudi bezgranične mogućnosti kreativnom umu u svetu zakonski dozvoljenog, tako kriminalci na internetu puštaju mašti na volju.

Druga glavna oblast nezakonitih radnji na Mreži jeste sajber industrijska špijunaža. Prema godišnjem izveštaju o pretnjama koji objavljuje Verizon, američki gigant na polju telekomunikacija, na nju otpada oko 34 odsto ukupne kriminalne aktivnosti na Mreži i skoro je sigurno da je najunosnija. Komunikaciona tehnologija doprinela je da je krađa industrijskih tajni lakša nego što je nekad bila. Dok kompjuteri nisu postali rasprostranjeni, krađa materijala podrazumevala je fizičku provalu u kompaniju ili, ako je posredi bio posao „iznutra", pronalaženje načina da se traženi podaci iznesu i predaju kupcu.

Takvih teškoća više nema: industrijski lopovi mogu da hakuju kompjuterski sistem korporacije i da potom pronjuškaju naokolo u potrazi za nacrtima, marketinškim strategijama, platnim

spiskovima ili bilo čime drugim što traže, i da onda prosto preuzmu te podatke. Dok još nije postao legendarni Iceman, Maks Vižn je radio duž cele Zapadne obale kao ispitivač upada – kompanije su mu plaćale da pokuša digitalni prodor u njihov sistem. Razgovarajući sa mnom u narandžastom kombinezonu, svojoj zatvorskoj uniformi, Vižn je rekao: „Tih godina postojala je samo jedna kompanija u koju nisam uspeo da provalim; to je bila vodeća američka farmaceutska kompanija." Što je i razumljivo – vrednost farmaceutskih kompanija leži u njihovim istraživanjima, a gubitak formula za nove lekove može da rezultuje finansijskim gubicima od više stotina miliona dolara i sunovratom cena deonica.

Vižn je bio besan kao ris zbog toga što nije uspeo da provali taj jedan sistem. „Dabome, tada sam pokrenuo fišing napad na njih i ušao sam u roku od pet minuta, ali to jednostavno nije bilo to." Pod time podrazumeva da je na imejl adrese kompanije poslao zaražene poruke, kad je bilo samo pitanje minuta pre no što neki od više hiljada zaposlenih upadne u zamku. Prema tome, čak i ako imate neosvojivu digitalnu tvrđavu, time ste prevazišli samo jedan od nekoliko glavnih bezbednosnih izazova.

Slično tome, zbog lakoće s kojom se podaci sakupljaju i skladište, ovih dana je mnogo lakše provaliti u kompaniju „iznutra". Znamo da je Bredli Mening, čovek optužen da je ukrao američke diplomatske depeše koje su docnije objavljene na sajtu Wikileaksa, uspeo da nareže ceo materijal na CD obeležen kao album Ledi Gage.

Znamo i da je Stuxnet – najsofisticiraniji kompjuterski virus do dana današnjeg – na navodni cilj u iranskom postrojenju za proizvodnju obogaćenog uranijuma morao podmetnuti (svesno ili nesvesno) neko ko je pomoću USB memorije ili CD-a zarazio njihov kompjuterski sistem. Naime, operativni sistemi iranskih nuklearnih postrojenja nisu povezani s internetom. Ali ipak čine mrežu, a njihova zaraza Stuxnetom dokazala je da su bili u dosegu profesionalne obaveštajne agencije.

Stuxnet je predstavljao značajnu eskalaciju treće glavne pretnje: sajber ratovanja. Taj konkretni malver je bio toliko složen, da su istraživači procenili da je za njegov razvoj bilo potrebno više godina rada, što znači da je posvećeni tim programera duže vreme morao raditi na njemu. Organizovani kriminal ne funkcioniše tako. Jedina sposobna da proizvede Stuxnet bila je država s mnogo resursa koje može da ulaže u osmišljavanje i

proizvodnju defanzivnih i ofanzivnih sajber oružja. Bez obzira na to, ko god da je proizveo Stuxnet, pozajmio je ogromne količine kompjuterskih kodova i tehnika od desetina hiljada crnih ili sivih hakera u sajberspejsu. Kriminalni hakeri su veličanstveni pokretač aktivnosti u svim oblastima na mračnoj strani Mreže. Vojska, privatni sektor, policija i obaveštajne službe vrlo brzo usvajaju oruđa koja razvijaju krakeri i hakeri.

Kad se Stuxnet uspešno infiltrirao u kontrolne sisteme nekoliko postrojenja za proizvodnju obogaćenog uranijuma u Iranu, vlasti su priznale da je to dovelo do velikog kvara u funkcionisanju krajnje osetljivog dela procesa, koji je mogao da rezultuje eksplozijom. Njegovo postojanje dokazuje da scenariji sudnjeg dana koje iznose takozvani sajber ratnici više nisu mogući samo u teoriji. Koliko god je u svoje vreme bio ozbiljan, napad na Estoniju bio je obično zagrevanje u poređenju s onim što najavljuje Stuxnet.

Sajber ratnike nazivaju i sajber sekurokratama – to su proroci što upozoravaju da će nam se nebo svakog časa sručiti na glavu. Među najrečitijima od tog soja je Ričard Klark, koji u svojoj knjizi *Sajber rat* (*Cyber War*) opisuje sledeći scenario:

> Kad stigneš u sedište Kriznog štaba, na drugom kraju bezbedne telefonske linije već te čeka direktor Agencije za odbranu informacionih sistema SAD (Defense Information Systems Agency, DISA).
>
> Federalna agencija za upravljanje u vanrednim situacijama (Federal Emergency Management Agency, FEMA) izveštava o velikim požarima i eksplozijama u rafinerijama u Filadelfiji i Hjustonu, kao i o smrtonosnim oblacima hlora koji se ispuštaju iz više hemijskih postrojenja u Nju Džersiju i Delaveru.
>
> U Nacionalnom centru za kontrolu leta u Herndonu, u Virdžiniji, u toku je potpuni kolaps svih sistema...

Većina sekurokrata nastavlja da tvrdi kako jedini način da sprečimo digitalni Perl Harbor ili Sajbergedon jeste da uložimo novac u njihove trustove mozgova i kompanije, kako bismo pojačali istraživanje i predupredili pretnju.

To se zapravo već dešava. Događaji u Estoniji ubrzali su pomeranje u pravcu militarizacije sajberspejsa. NATO je 2005. prvi

pristao da u Talinu, u Estoniji, obrazuje veličanstveno nazvani Kooperativni centar za sajber odbranu i nadmoć. Uprkos entuzijastičnom prihvatanju zamisli o operativnom instututu za sajber ratovanje, države članice su oklevale da izvade novac potreban u tu svrhu (s razumljivim izuzetkom zemlje domaćina, Estonije). Projekat nije odložen na neodređeno vreme, ali je imao velikih muka da dosegne fazu u kojoj je postao i nešto više od atraktivno dizajniranog papira sa zaglavljem.

„Međutim, čim je došlo do napada", primetio je Peter Lorens, ugledni estonski matematičar i jedan od suosnivača Centra, „atmosfera se promenila i iz Brisela i Vašingtona počela je da stiže stvarna podrška. Štaviše, moja prva reakcija na vest o napadu bila je da telefoniram u Francusku i poručim dva sanduka šampanjca 'kristal', s nalogom da ih isporuče gospodinu Putinu. Lansiranjem tog napada, Rusi su definitivno osigurali budućnost našeg centra."

U Vašingtonu je izvesno zvonilo na uzbunu. Događaji koji su neposredno prethodili estonskom incidentu ili se odigrali odmah posle njega ubedili su 2009. mladu Obaminu administraciju da je po svaku cenu potrebno pojačati sajber odbranu. Pogotovo je Agenciji za nacionalnu bezbednost, masivnoj američkoj operaciji globalnog nadzora, tek nekoliko meseci posle Estonije postalo istinski jasno koliko je ozbiljan gubitak predstavljao pad izviđačkog aviona EP-3E Aries u ruke kineskog vojnog vazduhoplovstva. Mada je pilot pre pada letelice uspeo da uništi softver, hardver je ostao neoštećen i Kinezi su se, čim su ga se domogli, poduhvatili rekonstruisanja vrhunske tehnologije koja će im omogućiti da prate i dekodiraju enkriptovane komunikacije. Ubrzo nakon ulaska Obame u Belu kuću, počeli su da testiraju svoju novu igračku, a Agenciji za nacionalnu bezbednost nije promakla njihova novostečena sposobnost da presreću komunikacije. Izgledalo je da Kinezi žele da daju Vašingtonu do znanja da su uspešno provalili tehnologiju.

Vlada Sjedinjenih Država nije se zaustavila na zalaganju za osnivanje centra za sajber odbranu u Talinu, koji od 2008. sprovodi obimna istraživanja koja obuhvataju i složene sajber vojne vežbe. Kompjuterske mreže postale su tako ključno važan deo infrastrukture Ministarstva odbrane i njegove ofanzivne i defanzivne operativne sposobnosti, da je državni sekretar za odbranu

Robert Gejts doneo izuzetno značajnu odluku da stvori novi vojni domen – sajberspejs.

Ovaj peti vojni domen – brat kopnu, moru, vazduhu i svemiru – jeste prva sfera vojnih operacija napravljena ljudskom rukom, a borbena pravila koja u njoj važe mutna su i skoro potpuno nerazumljiva. Sa tim domenom, Pentagon je osnovao i Sajber komandu SAD (United States Cyber Command, USCYBERCOM ili samo CYBERCOM), sa svrhom da nadzire neprijateljsku aktivnost u sajberspejsu i, ako je potrebno, razmesti ofanzivno naoružanje kao što je Stuxnet. SAD su trenutno priznati lider u pogledu sajber ofanzivne moći.

Ne bi trebalo brkati „sajber ofanzivnu moć" sa sposobnošću razmeštanja konvencionalnog naoružanja poboljšanog kompjuterskim sistemima. Najbolji primer ovog potonjeg arsenala jesu bespilotne letelice, takozvani dronovi (koje SAD redovno koristi u Avganistanu i Pakistanu), koje mogu da obavljaju izviđačke i borbene misije dok njima pilotira kompjuterski operater u Nevadi.

Sajber naoružanje čine hakerska oruđa koja sajber vojniku omogućavaju da prodre u kompjuterske sisteme *kritične nacionalne infrastrukture*, kao što su energetska i vodovodna mreža. Kad preuzme kontrolu nad sistemom, kaže se dalje u vojnoj doktrini, sajber zapovednik može da naredi njegovo zatvaranje (ili, kao što znamo iz priče o Stuxnetu, da izazove vrlo gadnu i opasnu eksploziju), usled čega će pogođeno društvo u roku od nekoliko dana biti svedeno na tehnologiju kamenog doba.

Tako barem glasi zamisao. Zasad su Sjedinjene Države priznate kao država koja prednjači u razvoju ofanzivnih sajber oružja. Međutim, za vratom im dahću Kinezi, Francuzi i Izraelci, a ni Indijci i Britanci ne zaostaju baš mnogo.

Militarizacija sajberspejsa mogla se predvideti. Kuda nas to vodi, međutim, to već niko ne ume da predvidi. Uvek proniclјivi Simor Herš je, u svom članku u *Njujorkeru*, uspeo je da dozna koje su implikacije toga što su Kinezi maznuli tajne sa hard diska izviđačke letelice:

> Debakl EP-3E dolio je u vojnim krugovima i Obaminoj administraciji ulje na vatru davnašnjeg spornog pitanja. Mnogi vojni lideri doživljavaju kineski upad kao upozorenje na sadašnje i buduće slabe tačke – na mogućnost da bi Kina ili neka druga zemlja mogle upotrebiti svoje sve veće sajber

veštine da napadnu američku civilnu infrastrukturu i vojni kompleks. Na drugoj strani su oni koji se zalažu za civilni odgovor na pretnju, usredsređen na širu upotrebu enkripcije. Oni se pribojavaju da će prekomerno oslanjanje na volju vojske imati negativne posledice po privatnost i građanske slobode.

Potreba vojske da se postavi kao glavni arbitar sajber sigurnosti je, izgleda, široko rasprostranjena. U oktobru 2010. predsednik Obama je zadužio Agenciju za nacionalnu bezbednost, koja je deo Pentagona, da pomogne Ministarstvu za nacionalnu bezbednost i privatnom sektoru u oblasti domaće sajber bezbednosti. U Kini, Narodnooslobodilačka armija je primarna institucija koja vodi računa o inostranoj i domaćoj sajber bezbednosti, dok su na Bliskom istoku Izraelske odbrambene snage nadahnuće za neverovatna istraživanja kompjuterskog ratovanja, koja Izraelu omogućavaju da na tom polju bude uticajniji nego što zapravo jeste.

Ali, neko će s pravom upitati, kakve sve to veze ima sa sajber kriminalom?

Pretnje u sajberspejsu su stvarne i opasne. Idealno, demokratska država bi trebalo da osigura da ova vitalno važna tehnologija bude građanima od koristi, a ne da im uništi život. Isto tako, država bi trebalo da se odupre iskušenju da krši naša prava i ugrožava nam privatnost. Uopšte nije pametno dozvoliti vojsci da preuzme vodeću ulogu u odbrani civilnih mreža. A opet, s obzirom na to da sajber oružja imaju potencijal da obogalje kritičnu nacionalnu infrastrukturu zemlje (i u procesu unište ljudima život), mora postojati zakonska odredba koja će omogućavati vojsci da u ekstremnim situacijama stupi u dejstvo. Te okolnosti morale bi biti vanredne i objektivne u isto vreme.

Za dejstvo protiv triju zasebnih pretnji – sajber kriminala, sajber industrijske špijunaže i sajber ratovanja – trebalo bi da budu odgovorne zasebne agencije. Priznate kriminalističke službe kao što su FBI i Tajna služba SAD trebalo bi da preuzmu odgovornost za rešavanje sajber zločina. Korporacije i kompanije trebalo bi da razviju sopstveni sistem bezbednosti mreže ili da za to plaćaju firmi specijalizovanoj za tu delatnost. Civilna vlada trebalo bi da uspostavi vlastitu odbranu mreže, dok bi vojska trebalo da štiti svoje sisteme.

Gledano spolja, sve to deluje dovoljno jasno. Međutim, u stvarnom svetu su ivice već zamućene, do čega je došlo usled interkonektivnosti Mreže. Zatim, tu je i dosad nerešiva dvodelna zagonetka u samom srcu sajber bezbednosti: kako izgleda sajber napad?

Da bi odgovorio na ovo, sajber branilac mora da poseduje dva osnovna saznanja. Odakle je potekao napad? I koji je napadačev motiv? Suočen sa veštim sajber agresorom, čak ni najbolji branilac ne može da odgovori na ta pitanja. Može samo da kalkuliše, a to – budući da dela na osnovu pretpostavke – može da dovede do pogrešnih odluka, nesporazuma i, naposletku, konflikta.

Pretpostavimo da se naša kriminalistička služba, korporativni sektor i vojska s dužnim poštovanjem pridržavaju zadatka da štite državu od opasnosti na koje su zaduženi da motre. Još uvek su tu dva igrača koja su uvek prisutna na spektru pretnji: tajni agent i haker. Prvi teži da reši zagonetku (mada ne nužno i da podeli ono što sazna); potonji je zapravo odgovoran za to što je zagonetka formulisana tako da bude nerešiva.

Obaveštajna agencija njuška po Mreži kao crna mačka pod okriljem mrklog mraka, nikad ne dajući ni glasa od sebe i družeći se samo onda kad njen tim želi da rastura, regrutuje ili zbuni. To fantomsko ponašanje deo je špijunske DNK, ali isto tako ga objašnjava fascinacija, pa čak i divljenje koje obaveštajna služba gaji prema svom najvećem protivniku u sajberu: hakeru.

Sve donedavno, mreža branilaca bila je ubeđena da se iza napada koji je u toku obavezno nalazi neki genijalni haker. To ubeđenje promenilo se za proteklih pet godina, s pojavom malvera „u slobodnoj prodaji". Mnogi hakeri kriminalci sada zarađuju ne petljajući s kreditnim karticama, bankovnim računima i sličnim lukavim šemama već prosto prodajom virusa, trojanaca i crva sopstvene izrade. To su programi jednostavni za korišćenje, koji ne iziskuju nikakvo specijalističko znanje. Najčešći vid je botnet. Botnete koji će se koristiti u DDoS napadima, u svrhe kao što su iznuda ili osveta, hakeri iznajmljuju na dan ili dva, možda na nedelju ili mesec dana. Normalno, hakeri koji prodaju botnet ili virus poseduju tehničko znanje potrebno da kontrolišu trajanje perioda iznajmljivanja, zato što im prosto uprogramiraju rok zastarevanja, a njihovi klijenti - po svoj prilici sitni lopovi – tu ne mogu ništa.

Ipak, pojava sekundarnog tržišta na netu, za malver u „slobodnoj prodaji", neće promeniti fundamentalnu istinu da iza

svakog sajber napada – bilo da je posredi kriminal, industrijska špijunaža ili ratovanje – stoji talentovani haker. Pokretanje sajber napada koji nisu samo nezgodni već nanose istinsku štetu neosporno zahteva visoko specijalizovano tehničko znanje. To znači da haker – čak i ako radi za nekakvog šefa (bio to *capo*, generalni direktor kompanije ili vojni zapovednik) – *ako* hoće da dizajnira odgovarajući proizvod, i dalje mora mnogo da zna o meti koju je naciljao. Na primer, bez obzira na to koji je hakerski tim dizajnirao Stuxnet, morao je da zna ne samo o iranskim nuklearnim postrojenjima koja su bila pretpostavljeni ciljevi: morao je da se razume i u Siemens PLC mrežu koja je upravljala njima i u vrlo specifičnu kompresiju koju je dizajnirao finski Vachon (iako je softver proizveden u Kini), kao i da zna za tajvansku kompaniju čiji je digitalni sertifikat RealTek spufovan kako bi prevario antivirus program iranskog sistema.[36] Svako dovoljno pametan da radi na Stuxnetu izvesno je dovoljno pametan i da prouči žrtvu na koju se namerio.

U tom pogledu, ključ sajber bezbednosti su hakeri, pošto oni znaju rešenje zagonetke. Nađite hakere i napravićete značajnije korake prema otkrivanju istine.

Ogroman procenat finansijskih sredstava koje vlade sad usmeravaju u sajber bezbednost posvećen je „digitalnim rešenjima" – bore se gedžetima protiv gedžeta. Za razumevanje hakera, njihove kulture, njihovog uma, njihovih namera i slabih tačaka izdvajaju se zanemarljive sume novca. Ali kako da pronađete hakera? A kad ste na internetu, kako da znate je li vaš novostečeni prijatelj haker, policijski špijun, obaveštajni agent, istražitelj Vazduhoplovnih snaga, obešenjak, terorista ili vanzemaljac?

Sve se vrti oko poverenja. A izgradnja poverenja podrazumeva strpljivost i negovanje odnosa. Ipak, u svetu sajber bezbednosti, vreme je dragoceno. Teškoće vezane za poverenje i vreme nikad mi nisu postale tako jasne kao onda kad se „lice mesta" Dark-Marketa odmaklo daleko od njegovog nastanka u Britaniji, Nemačkoj i Sjedinjenim Državama, prema zemlji čiji ekonomski i geostrategijski značaj veoma brzo raste – Turskoj.

36 Spufovanje (eng. *spoofing*): u kontekstu mrežne bezbednosti, napad spufovanjem je situacija u kojoj se jedna osoba ili program uspešno maskira kao druga, tako što falsifikuje podatke i time stekne nezakonito preimućstvo. (Prim. prev.)

KNJIGA DRUGA

Deo I

26.
Bilal u Pitsburgu

Pitsburg, Pensilvanija, februar 2008.

Jednog hladnog zimskog jutra 2008. inspektor Bilal Šen iz turske policije gledao je kroz prozor svoje kancelarije u pitsburški most Usijani metal. Opkoračujući reku Monongahela samo malčice južnije od mesta gde se ona spaja s Alegenijem i obrazuje veličanstvenu reku Ohajo, most je nekada služio za transport istopljenog metala iz velike visoke peći Elajza na severnoj strani do valjanonica na južnoj.

Danas, međutim, nije imao vremena da razmišlja o postindustrijskoj estetici snegom pokrivenog Pitsburga. Na forumima DarkMarketa je upravo pročitao nešto uznemirujuće. Prema navodno pouzdanim informacijama koje su potekle iz Istanbula, ChaO, jedan od sajber kriminalaca pod istragom inspektora Šena, bio je „jedan od glavonja, bogat i moćan". Turčinu je bilo lako da dešifruje ovu frazu: meta je imala prijatelje na visokim položajima, noćna mora svakog turskog policajca.

Inspektor Šen je već skoro tri meseca radio u Nacionalnoj alijansi za obuku sajber forenzičara. Prvog dana, dok je na recepciji čekao da ga primi šef organizacije, slučajno je ušao Kit Dž. Mularski, vedar i šarmantan kao i uvek. Predstavio se i, čuvši da je Bilal iz Turske, odmah je počeo da mu priča sve što je znao o čoveku s nadimkom ChaO, ozloglašenom administratoru DarkMarketa i vodećem kriminalcu. Mularski i Šen su odmah „kliknuli".

Kad je ušao u poslovne prostorije na četvrtom spratu zgrade u Tehnološkoj ulici 2000, turskom policajcu je palo u oči da više liče na kancelarije osiguravajućeg društva nego na užurbano haj-tek okruženje poznato iz serija kao što je *Mesto zločina: Njujork* (*CSI: New York*). Jedna zabačena prostorija bila je prepuna instrumenata

za kompjutersku forenziku, mašina kadrih da izvuku i najskrivenije tajne svake digitalne naprave. Međutim, ta sala za tehnološka ispitivanja bila je jedva vidljiva i potpuno izolovana, kako bi se sprečilo da neki trojanac ili kakav drugi malver kontaminira predmete pod istragom (jednako kao i njihovi organski pandani, kompjuterski virusi se ponekad prenose putem vazduha). Ako se to ostavi po strani, poslovne prostorije su bile tihe, uredne i neupadljive.

Tog prvog prepodneva, Kit je Bilalu pokazao belu tablu u svojoj kancelariji, s imenom „ChaO" na vrhu piramide kriminalaca povezanih sa DarkMarketom. Ušavši, turski policajac se postideo. Uz podršku kolega iz Britanije i Nemačke, federalci su pre šest meseci uhvatili dva najenergičnija administratora, JiLsija i Matrixa. Hapšenja je bilo u Britaniji, Nemačkoj, Kanadi i Francuskoj, a spremala su se i nova, u Sjedinjenim Državama. Stoga je policajac iz Ankare činjenicu da se jedan Turčin nalazi među najtraženijim sajber kriminalcima na svetu doživeo kao mrlju na nacionalnom ponosu ali i na svom ugledu.

Turska policija, a pogotovo njen odsek za organizovani kriminal, mnogo su napredovali u odnosu na prethodnu deceniju, i Bilal je bio rešen da dokaže da je nedavno oformljena Jedinica za sajber kriminal, sa sedištem u turskoj prestonici Ankari, sposobna da zaigra u velikoj ligi i pored toga što raspolaže mnogo manjim resursima.

U prostorije FBI-ja stalno su navraćali policajci iz celog sveta. Dolazili su da uče od američkih kolega, ali i da grade mreže uzajamne pomoći. Saradnja među policijama različitih zemalja obično stenje pod pritiskom nepodnošljivih birokratskih procedura, a najbrži način da se to prevaziđe jesu lična prijateljstva među policajcima.

Bilal je došao na tri meseca. Kao Turčin, bio je nov, mada potencijalno vrlo koristan kontakt za federalce. Godine 2003. bio je jedan od dvojice osnivača malobrojne Jedinice za sajber kriminal u turskoj Upravi za borbu protiv krijumčarenja i organizovanog kriminala. A u poređenju s prestupnicima, inspektor nije imao nikakvih resursa.

Što se njega samog ticalo, Bilal Šen je želeo da uči od FBI-ja. Doduše, nije bio baš neiskusan. U policiju je ušao 1989, kao petnaestogodišnjak, upisavši se u napornu osmogodišnju policijsku školu – najduža policijska obuka u svetu. Bilo je pomalo

čudno jer je inspektor Šen, omalen i obziran u ophođenju, više podsećao na turskog Herkula Poaroa nego na tradicionalnu sliku žilavog balkanskog policajca, ogrubelog od baktanja sa provincijskim banditima, urbanim narko-sindikatima i nehumanim krivično-pravnim sistemom.

Policijska akademija se ispostavila kao naporan režim. Međutim, ono što je Bilalu najteže padalo nije bio spartanski nameštен studentski dom ili nemilosrdna obuka umnogome nalik vojničkoj već potpuno odsustvo kompjutera. Još kao dečak koristio je svaku priliku da se ušunja u lokal s arkadnim igricama u svom rodnom gradu Eskišehiru, smeštenom u severnoj Anadoliji, na sredokraći između Istanbula i Ankare. Imao je samo šest godina kad je naišao na igricu *River Raid*. Svaki slobodan minut provodio je leteći uzvodno dvodimenzionalnim borbenim lovcem, pucajući na malene helikoptere, brodove, tenkove i dirižable, i pokušavajući u isto vreme da dopuni rezervoar gorivom. Obuzet tom tajanstvenom fuzijom ponavljanja i povremene nagrade koja toliku decu, adolescente i mlade odrasle ljude drži prikovane za kompjuterski monitor, Bilal je bio opsednut igricama kao i mnogi proto-hakeri njegovih godina. Isto tako, bio je obuzet podjednakom rešenošću da pobeđuje.

Možda je baš ta tvrdoglavost pomogla neiskusnom novajliji na njegovom prvom radnom mestu, seoskoj policijskoj stanici usred anadolske nedođije. Mada je bila sredina devedesetih, najsofisticiraniji uređaj u njoj bila je prastara pisaća mašina. Smatralo se da je uzimanje izjava od svedoka nedostojno njegovog položaja, ali Bilal je bio u toj meri rešen da dobro nauči da kuca da je provodio sate i sate nad tastaturom. A kad se nije bavio time, taj neverovatni samouki čovek je bez ičije pomoći učio mandarinski kineski jezik.

Kad je podneo molbu za prijem u elitnu Jedinicu za organizovani kriminal u Ankari, tamošnji starešina je upitao Bilala zašto uči kineski. „Pošto se Kina otvara prema spoljnom svetu", odgovorio je ovaj, „uskoro će nam u Odseku za organizovani kriminal biti potrebni oni koji govore taj jezik." Taj odgovor bio je presudan da ga prime.

Našavši se u turskoj prestonici, mladi detektiv upisao je master studije na Univerzitetu u Ankari, opet o svom trošku i u slobodno vreme. Odabrao je temu koja je u Turskoj bila nepoznata i neproučena – „Mogućnosti i rizici elektronske uprave" – u kojoj

je razmotrio odnos između privatnosti, građanskih prava i sajber kriminala.

Bilal Šen je počeo da prati širenje internet kriminala u svojoj zemlji, kao jedan od malobrojnih turskih policajaca koji je posedovao kapacitet za to – jedini drugi državni organi koji su već bili svesni strategijske važnosti sajber bezbednosti bili su vojne i civilne obaveštajne službe, ali one, dabome, nikad ne udaraju svoje mogućnosti i motive na sva zvona.

Sa jednim kolegom, Bilal se latio herkulovskog zadatka da ubedi glomazno Ministarstvo unutrašnjih poslova da preusmeri delić svojih dragocenih fondova u osnivanje Jedinice za sajber kriminal. Bile su im potrebne tri godine preklinjanja, nagovaranja i vođenja kampanje. Srećom, imao je saradnika koji je majstorski vladao osmanlijskom umetnošću naštimavanja pravog tona s odgovarajućim birokratama u Ministarstvu unutrašnjih poslova.

Kao što je to bio slučaj i s ostalim jedinicama za borbu protiv sajber kriminala što su nicale u kriminalističkim službama širom sveta, ovaj novi odsek u Turskoj uspeo je da iskoristi činjenicu da takoreći niko drugi u ministarstvu nije shvatao tamnu stranu kompjutera. Kad su dobili odobrenje, njih dvojica su se osetili nekako oslobođeni svakog mešanja sa strane, budući da niko nije imao predstavu šta rade, a baš se i nije moglo reći da predstavljaju opterećenje za državnu blagajnu.

I dok je inspektorova rođena vlada jedva bila svesna njegovog rada, njegove kolege preko Atlantika su vrlo brzo primetile njegove uspehe. U leto 2007, kad je policija u Nemačkoj i Britaniji uhapsila administratore DarkMarketa, JiLsija i Matrixa001, turski tim za borbu protiv sajber kriminala stavio je iza rešetaka jednog od najzloglasnijih sajber kriminalaca, Maksika. Maksim Jastremski iz Harkova, grada na severoistoku Ukrajine, glavni igrač na DarkMarketu (između ostalih, snabdevao je „dampovima" Lorda Kaisersosea, francuskog hakera iz Marseja), pretpostavio je da će u Turskoj biti bezbedan – ne samo da tamo nikad nije uhapšen nijedan sajber kriminalac, već ni odnosi između Ukrajine i Turske nikad nisu bili srdačniji, pogotovo u podzemlju.

Ukrajinci su ovu zemlju obožavali i zbog njene veličanstvene obale – prelepe plaže Antalije postale su obavezna destinacija sajber lopova iz obeju država.

Tajna služba SAD je već dve godine pratila Maksika. Dve hiljade šeste uspešno su ukrali tajne s njegovog laptopa i potom organizovali sastanke između njega i svog tajnog agenta na Tajlandu, u Dubaiju i u Turskoj. U prošlosti se saradnja s turskom policijom pokazala kao nezgodna, ako ne i potpuno nemoguća. Međutim, hapšenjem Maksika dok se baškario na bleštavom suncu Antalije, turska policija poslala je signal da je, što se tiče sajber kriminala, spremna da sarađuje i da zna kako da to uradi.

Premda JiLsiji i Matrixi ovog sveta nisu više krstarili forumima DarkMarketa, ostatak ekipe je još bio aktivan – štaviše, DarkMarket je doživljavao porast kriminalne aktivnosti. Ironijom sudbine, ključ tog oživljavanja ležao je u hapšenju još jednog sajber kriminalca: Icemana.

U septembru 2007. američka policija je konačno ušla u trag Maksu Vižnu u njegovom skloništu, stanu u centru San Franciska. Icemanov odlazak izazvao je urušavanje CardersMarketa i tako je, dok je *mazafaka* kontrolisala rusku karding scenu, DarkMarket sada bio neosporeni šampion sajber kriminalaca s engleskog govornog područja. Direktno ili indirektno, sajt je još generisao stotine hiljada funti nezakonitog profita svakog meseca, pa je među karderima i hakerima bio popularniji nego ikad.

Na DarkMarketu su sad postojala tri ključna igrača: ChaO, Master Splyntr i Shtirlitz, a uskoro će im se priključiti i tajanstveni Lord Cyric. Cyricovo prisustvo na karding sceni generisalo je među karderima mržnju i obožavanje u jednakoj meri. Oni koji su ga se gnušali verovali su da je on ubačeni agent FBI-ja, Mularski, mada je bilo sumnji da zapravo Master Splyntr i Shtirlitz rade za tu američku kriminalističku službu ili sa njom. Postojalo je, međutim, nešto u vezi s čime su svi bili jednoglasni, a to je da je ChaO, bio on pandur ili haker, najozbiljniji krimos koji je ostao na forumu.

Za razliku od sve debljih dosijea o njegovim kolegama DarkMarketarima, Mularski i Šen su o samom ChaO-u znali samo dve važne činjenice: da živi u Istanbulu i da vodi uspešan biznis prodaje takozvanih „skimera", tog esencijalnog oruđa za prevarante u Dobu plastike. Međutim, detektivi nisu znali njegovo pravo ime, kao ni fizičku adresu, IP adresu niti ikakve poznate saradnike. Ili ChaO nije postojao (što nije bilo nemoguće), ili nikad nije grešio.

Ako je posredi bilo potonje, tada je izgledalo da je ChaO usavršio sistem zavaravanja svojih digitalnih tragova u toj meri da je forenzičkim istražiteljima bilo nemoguće da ustanove njegovu lokaciju. Deo tog sistema zavaravanja traga obezbedio mu je Grendel, koji je u slobodno vreme pomagao DarkMarketu (naplaćujući svoje usluge pouzećem). Ironija je bila u tome što je on istovremeno obezbedio i sistem ljusaka koji je maskirao lokaciju servera Mularskog. JiLsi je bio prvi koji je pozvao Grendela da pruža DarkMarketu tu vrstu usluga – Grendel je, naime, u stvarnom životu radio za nemačku firmu koja se bavila IT bezbednošću. Jeste bilo ironično, ali nekako je baš i ličilo na DarkMarket, to što je na kraju putem tog sajta pružao usluge i kriminalcima i policajcima.

Uprkos intenzivnim naporima, Bilal Šen nije uspeo da spoji ChaO-v stil (ili *modus operandi*, kako je to policija nazivala) ni sa jednim poznatim kriminalcem u Turskoj. Izgledalo je kao da su u njegovoj ličnosti koincidirala dva fundamentalna aspekta mračne strane interneta: bio je gik koji je posedovao zadivljujuće tehničko znanje, ali i talentovani kriminalac koji je sve planirao do poslednjeg detalja i ništa nije prepuštao slučaju. Takođe je bilo moguće i da je ChaO kolektivno ime dobro organizovane kriminalne grupe, mada je lingvistička analiza snažno nagoveštavala da sve njegove postove i poruke na internetu formuliše jedna te ista osoba.

Stoga, kad je Bilal dobio iz Istanbula poruku da je ChaO „jedan od glavonja", ne samo da se zabrinuo nego je i znao da će od tog trenutka morati dobro da pripazi šta radi, čak i u zemlji koja se modernizovala tako brzo kao Turska.

Posle smene milenijuma, Turska je postala sve privlačnije poprište za hakere, krakere i sajber kriminalce. Potkraj devedesetih, veliki deo sajber kriminalne aktivnosti grupisao se u određenim regijama takozvanih zemalja BRIK-a. Ekonomista iz Goldman Saksa skovao je ovaj akronim za Brazil, Rusiju, Indiju i Kinu kao vodeće zemlje novih tržišta, drugi red globalne moći posle G8 (mada Rusija politički pripada i jednima i drugima).

Zemlje BRIK-a delile su određene društvene i ekonomske karakteristike. Njihove privrede su dobijale zamah i otvarale se posle višedecenijske stagnacije. Imale su brojne populacije, čiji su udruženi napori registrovali visoku stopu rasta, dok je prelazak u status dinamičnog globalnog igrača pratilo uskrsavanje nabujalog

i katkad agresivnog nacionalizma. Njihovi obrazovni sistemi nudili su odlična osnovna znanja. Međutim, udruženo s krajnje nejednakom raspodelom bogatstva, ovo je iznedrilo novu klasu mladih ljudi, siromašnih i nezaposlenih, ali – za razliku od ranijih generacija – s velikim materijalnim težnjama, budući da su upijali potrošačke poruke koje su neodvojivi, suštinski deo globalizacije. Da bi ostvarili te težnje, jedan manji broj njih počeo je vredno da radi u internet kafeima, gde su bili sigurni da ih neće primetiti policija, ali ni iko drugi, što se toga tiče, i gde su pronalazili bezbroj onlajn mogućnosti da nauče hakerski zanat.

Turska se kvalifikovala kao počasna članica BRIK-a, s privredom koja je delovala mnogo dinamičnije u poređenju s, recimo, ruskom. Pri tom su se njena populacija od oko osamdeset miliona i razvojne stope povećavali još brže od onih u punopravnim članicama BRIK-a. Svi su priznavali strategijsku važnost Turske, onako ugnežđene među obalama Crnog i Sredozemnog mora i s granicama prema Bugarskoj, Grčkoj, Iranu, Iraku, Siriji i Jermeniji: ta zemlja gotovo da nema nijednog suseda koji za poslednje dve decenije nije doživeo neki veliki unutrašnji potres. Nepredvidljivo je oduvek prisutno u turskoj politici, ali, sa smenom milenijuma, narastajuća ekonomska moć i sofistikacija Turske istakli su njenu središnju ulogu u nekoliko vitalnih geostrategijskih regiona – na Bliskom istoku, u Centralnoj Aziji, na Crnom moru i na Balkanu.

Zemlja je devedesetih sporo razvijala svoju internet strukturu, ali poslednjih godina je naglo počela da hvata korak. Njen privredni centar, Istanbul, bio je domaćin pravoj eksploziji uspešnih novih kompanija u oblasti tehnologije, kao i dizajnerskim i medijskim kompanijama i firmama za uslužne delatnosti, kojima je takav razvoj išao na ruku.

Loša strana je bila ta što su veličina zemlje, njena sve bolja infrastruktura i sve šire obrazovanje mlade srednje klase predstavljali odličnu priliku za sajber kriminal. Sve do 2005, kad je jedinica Bilala Šena proradila punom parom, malo je toga sprečavalo hakere i krakere u Turskoj da operišu na Mreži bez straha da će biti otkriveni. Jedinica za sajber kriminal počela je da menja tu situaciju, ali bio je to sizifovski napor. Ako inspektor Šen uspe da uđe ChaO-u u trag, to će biti važan trofej za njegovu jedinicu.

Međutim, baš uoči povratka iz Pitsburga u Tursku sredinom marta 2008. dobio je još jedno upozorenje koje je dodatno

iskomplikovano njegovu istragu ChaO-a. Ovog puta su mu njegovi istanbulski kontakti dostavili pojedinosti zbunjujućeg intervjua što ga je poznatoj medijskoj kući *Haber 7* dao turski haker s nadimkom Kier, koji je priznao da je begunac od zakona.

Reputacija *Habera 7* temelji se delom na duhovnoj podršci koju dobija od velikog domaćeg islamističkog pokreta pod nazivom Gulen, koji promoviše filozofiju svog vođe Fetulaha Gulena koji živi u egzilu u Sjedinjenim Državama. Kao medijska agencija pokreta, *Haber 7* je naklonjen vladajućoj AK partiji,[37] koja je proislamska ali demokratska.

Mladi haker Kier obratio se ovoj medijskoj kući s tvrdnjom kako ne samo da poznaje ChaOa, već i da, kako je nagovestio, osoba ili ljudi iza najuspešnijeg tajanstvenog avatara DarkMarketa planira/ju širenje svoje kriminalne imperije. U članku se nalazila i fotografija hakera, snimljena za vreme razgovora u jednom istanbulskom kafiću – s leđa, doduše, ali se ipak video deo profila.

Bilal još nije znao da je taj haker mladić po imenu Mert Ortač. Verovalo se da je taj čudni lik saučesnik drugog sajber kriminalca zvanog Cryptos, koji je u januaru 2008. uhapšen pod optužbom da je hakovao Akbank, jednu od najvećih finansijskih institucija u Turskoj. Akbank je u mnogome bio nešto još veće od DarkMarketa, zato što se ta ekipa uhakovala u glavni sistem banke, iskoristivši slabe tačke njenog operativnog sistema. Međutim, ni istanbulska policija ni Uprava za borbu protiv organizovanog kriminala nisu imali ni najbleđu predstavu gde se krije Ortač. A onda je ovaj naglo iskrsao odnekud i razgovarao s novinarom.

Uprkos tome što se nalazio pod prismotrom policije i čitave čete obaveštajaca, rekao je Ortač novinaru, u decembru 2007. im je svima pobegao i otišao u ilegalu. Iz nje je izašao samo taj jedan put, da ispriča novinama svoju čudnu i nepotpunu priču.

Istanbulska policija bila je osramoćena ovim njegovim kameo pojavljivanjem. Implikacije intervjua – lakoća s kojom je izbegavao hapšenje – bili su uznemirujući. Koliko da natera policiju da se oseti još bednije, haker ih je upozorio da hapšenja u slučaju Akbank neće imati nikakvog uticaja na bezbednost turskih banaka zato što ih jedan mnogo gori kriminalac trenutno maksimalno „guli" – a njegovo ime je ChaO. (Bilal Šen je, dabome, već pre toga čuo za njega, ali ovo je bio prvi put da se ChaO javno pominje – i to od strane tajanstvenog muškarca.)

37 Kod nas poznata kao Partija pravde i razvoja. (Prim. prev.)

Ortač je izneo tvrdnju da se ChaO nalazi pod zaštitom državnih zvaničnika. Što se Šena ticalo, taj intervju je u najmanju ruku predstavljao potvrdu da ChaO postoji. Bez obzira na to, nakon što ga je pročitao, inspektora je obuzeo osećaj da stoji na samom rubu provalije. Ko je taj što štiti ChaO-a, i zašto?

27.
Visoka porta

Podigavši pogled sa svojih beležaka, inspektor Šen je osećao kako se njegova nelagoda postepeno preobražava u strah. Kako se činilo, sada je ChaO glavom, reagujući na Ortačev intervju, poslao poruku informativnom kanalu *Haber* 7. Bio je to nečuveni izliv besa, začinjen žestokom dozom megalomanije i gvozdenog ubeđenja. „Ja sam najviši zakon na DarkMarketu", grmeo je. „Ja sprečavam delovanje policije i deratora. Ja diktiram pravila, a ostali ima da ih se pridržavaju."

Inspektorovi kontakti ubrzo su nagovestili kako je vrlo moguće da je ChaO iznad zakona. Šen je popričao sa svojim najstarijim prijateljem u istanbulskoj policiji. Situacija je bila zastrašujuća: obojica su se pribojavali da ChaO možda ima doušnika u policijskim redovima, nekoga ko će, razume se, obaveštavati svoga gazdu o napredovanju istrage. A ako ne mogu da veruju svome timu, svojoj podršci i, što je najvažnije, svojim pretpostavljenima, kako da onda ostvare ikakav napredak u ovom slučaju?

U prvom intervjuu, Mert Ortač je mnogo pričao o tajnoj policiji i drugim silama na delu u slučaju DarkMarketa. Tako nešto bi u drugim zemljama možda vonjalo na paranoju o zaveri, ali u Turskoj ne bi bilo mudro sasvim odbaciti to kao bulažnjenje. Mert je nagovestio da bi cela operacija DarkMarket mogla dotaći ljude u samom vrhu ekonomske ili političke vlasti.

Komplikovana politička struktura zemlje poprimila je novi oblik otkako je AKP na izborima 2002. postala dominantna sila. S obzirom na to da više od 90 odsto Turaka čine muslimani, činjenica da je otvoreno muslimanska partija odnela glatku pobedu nije bila iznenađujuća sama po sebi. AKP je insistirala da je njena odanost veri na drugom mestu u odnosu na posvećenost demokratiji, baš kao što mnoge umereno konzervativne partije u Evropi nazivaju sebe *hrišćanskim* demokratama.

Međutim, Turska se diči još jednom neizmerno snažnom ideološkom tradicijom – kemalizmom. Nazvan po osnivaču moderne

Turske, Kemalu Ataturku, kemalizam je doktrina čiji vodeći princip propoveda potpuno razdvajanje crkve i države. Univerzalno prisustvo Ataturkovog lika u izlozima, porodičnim domovima, kancelarijama, kasarnama, bolnicama i zatvorima odražava duboko poštovanje koje Turci gaje prema njegovoj baštini sekularizma (kao i strah od hapšenja ukoliko se ne povinuju).

Kemalizam, međutim, dolazi u najrazličitijim ukusima. Njegove dve najvatrenije grupe sledbenika potiču iz svetovnih elitnih krugova srednje klase: intelektualci, profesionalci i državni službenici s jedne i takozvana Država u državi s druge strane. I jedni i drugi su podozrivi prema AKP.

Država u državi je primereno zlokoban naziv za vojno-industrijski kompleks koji u posleratnom periodu deluje kao vrhovni arbitar turske politike. Kao jedna od samo dveju članica NATO-a koja se graničila sa Sovjetskim Savezom (druga je bila Norveška), zemlja je odigrala ključnu ulogu u Hladnom ratu, a njeni saveznici, na čelu sa SAD, rado su se pravili da ne vide nečuvena zlostavljanja koja je turski narod trpeo od sopstvene vojske.

Za vreme svog stalnog mešanja u politički život, bezbednosni establišment Turske zario je zube duboko i u privredu zemlje, sve dok povremeno nije postalo teško razlikovati grabljivca od plena. Svoje razgranato i lukrativno mešanje štitio je pozivanjem na kemalizam: ako mu se učini da mu krhki demokratski poredak ugrožava poslovne interese, intervenisala je vojska, s izgovorom da mora da zaštiti Ataturkovu baštinu. Po tradiciji, oružane snage nisu dozvoljavale nikome i ničemu da im stoji na putu. Da parafraziramo staru tursku poslovicu: „Pružiš li ruku Državi u državi, otkinuće ti je do ramena."

Međutim, vlade koje su se poslednjih petnaestak godina redale u Turskoj uvele su niz reformi, delom u pokušaju da ispune kriterijume za članstvo u Evropskoj uniji. Bez obzira na strahove da imaju skriveni ekstremistički islamistički program, novi vladari iz AKP uveli su u tursko društvo neke vrlo liberalne promene, kao što je abolicija smrtne kazne. U drugom pokušaju da konsoliduje primat vladavine prava, AKP razdvaja redovne policijske snage zemlje od vojnih.

Taj proces doveo je do nekih upečatljivih i vrlo pozitivnih promena. Delovi državnih službi počeli su da shvataju kako njihov primarni zadatak nije da pune sopstvene džepove nego da

služe narodu, kao i da efikasno funkcionisanje turske države poboljšava njen međunarodni uticaj i povećava joj ugled.

Međutim, spori proces rađanja nove Turske nije bio bezbolan, niti je ishod ikad bio predvidljiv. Prati ga titanska politička borba u kojoj promena savezništava među netransparentnim snagama ume da se ispostavi kao kobna za svakog ko se, namerno ili nenamerno, nađe između njih.

Glavno poprište rata među tim snagama zvanično je otvoreno 2007. pokretanjem takozvane istrage Ergenekon. Ergenekon, inače naziv epa u kome je opevana prastara turska legenda, u novije vreme je ime navodne zavere Države u državi, u kojoj su vodeće vojne, obaveštajne i političke ličnosti sarađivale s organizovanim kriminalom, novinarima, advokatima i drugim profesionalcima. Cilj im je, navodno, bio da ograničavaju uticaj demokratski izabranih vlada, pogotovo AKP. Međutim, prema tužiocima i medijima naklonjenim vladi, zavera je išla i dalje od toga – pripadnici organizacije Ergenekon planirali su 2009. vojni puč, kako bi povratili vlast Države u državi nad izabranom vlašću.

Od 2007. policija je u takozvanim Ergenekon „talasima" pohapsila stotine viših vojnih oficira i zvaničnika obaveštajne službe. Međutim, s njima su uhapsili i desetine novinara i advokata koje optužuju da su iz koristoljublja ili zbog ideologije sarađivali s Ergenekonom. Malobrojna ali elokventna klasa liberalnih intelektualaca i mnogoljudnija srednja klasa upozoravaju da demokratska vlast pribegava nekoj vrsti zastrašivanja, kakva se obično povezuje sa Državom u državi. U skladu s vremenima, optužnica protiv Ergenekona se najvećim delom oslanja na digitalne dokaze – prisluškivanje mobilnih telefona, praćenje komunikacije preko mesindžer servisa i kompjuterski fajlovi, demonstrirajući tako narastajuće sajber kapacitete domaćih obaveštajnih službi.

Bilal Šen nije imao nikakvu ulogu u tim dešavanjima, osim što su ga njegova marljivost, posvećenost i mladalačka energija pre svrstavali na stranu nove, a ne stare Turske. Ipak, poput većine Turaka, bio je duboko svestan osetljivog političkog konteksta u kom rade on i svi ostali. Nijedan turski policajac nije želeo da postane nedužni pion koji će nastradati u bici između Države u državi i demokratski izabrane vlasti. Skoro svi Turci su, ako su ikako mogli, izbegavali da u javnosti raspravljaju o Ergenekonu. Međutim, svi su znali da ta istraga lebdi u pozadini mnogih

važnih krivičnih postupaka, bez obzira na to da li oni sadrže otvorene političke implikacije.

Bilal je znao da mora da vodi računa, ali nije imao nameru da odustane od potere.

Dok je boravio u Pitsburgu, između njega i Mularskog rodilo se snažno prijateljstvo, a agent FBI-ja preneo mu je sve informacije koje su uspeli da skupe o ChaO-u. Njih dvojica počeli su da sastavljaju oskudni dosije. Mularski je bio u situaciji da izvadi podatke iz svoje ogromne arhive, a Šen je umeo da čita turske rune. Inspektor je želeo da dobije sliku o ličnosti ChaO-a, da vidi poklapa li se s nekim od sajber kriminalaca u njegovoj zemlji: prečešljali su gomilu dokumenata, a onda ih slali tamo-ovamo na relaciji između Ankare, Istanbula i Pitsburga.

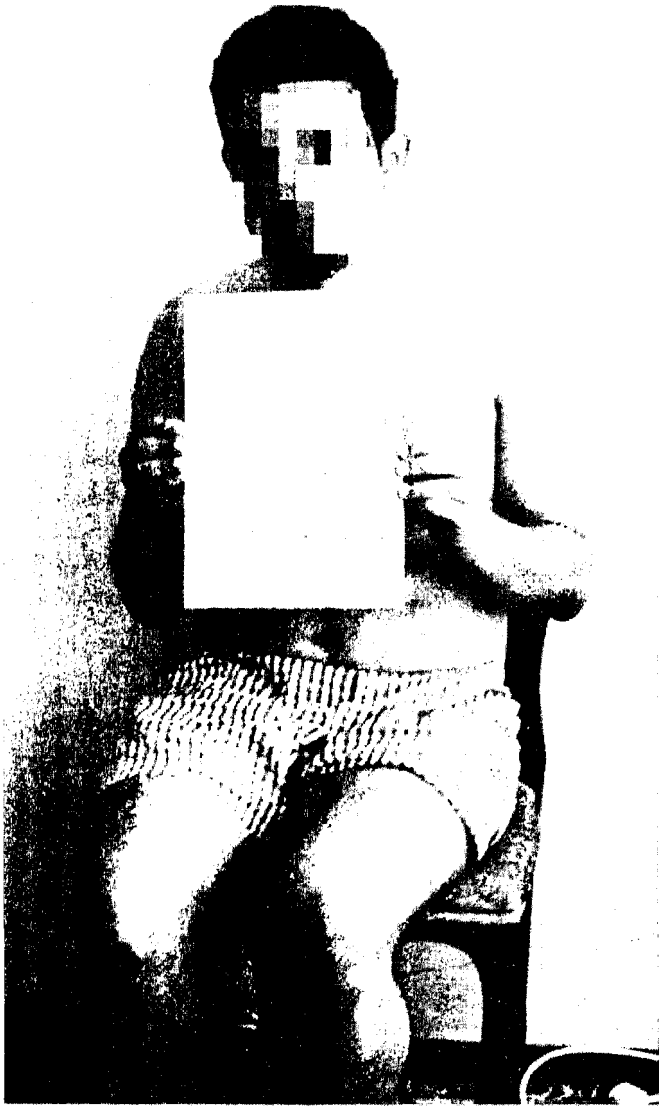
A kao da situacija već nije bila dovoljno zbunjujuća, ubrzo nakon što se inspektor Šen vratio kući u Ankaru, došlo je do još čudnijeg zaokreta. Mrežom je kružila čudna slika.

Bilal je jedva uspevao da suspregne svoj gnev i osujećenost. Agent Mularski mu je poslao fotografiju koja se pojavila na sajtu *Habera 7*, a potom i u časopisu *Wired*, sa sedištem u San Francisku. Tajanstveni muškarac Kier je sedeo na stolici, u donjem vešu, primoran, kako je izgledalo, da drži list papira na kom je pisalo:

1 JA SAM KIER. PRAVO IME MI JE MERT ORTAČ
2 JA SAM SARADNIK MEDIJA
3 JA SAM TASTER. JA SAM KLJUN.
4 JA SAM REPORTER
5 ChaO ME JE KRESNUO

Pola istanbulske policije uzalud je tragalo za Kierom – ili Mertom Ortačem, da mu damo njegovo pravo ime – ali ChaO je uspeo ne samo da ga nađe nego i da ga otme i izvrgne poniženju. Bilo je savršeno moguće da je čoveku život u opasnosti. Šta se to dešavalo?

Po shvatanju Bilala Šena, bilo je samo po sebi razumljivo da ništa što ima veze sa Mrežom nije pametno uzimati zdravo za gotovo. Kao iskusni surfer po kriminalnim forumima i proučavalac ponašanja ljudi na internetu, znao je da je sasvim normalno da



lažu, varaju, preteruju, obmanjuju i kuju zavere. Međutim, istorija DarkMarketa u Evropi, a pogotovo u Turskoj, išla je još dalje od ove uobičajene dvoličnosti i evoluirala u nadrealnu priču o mahinacijama, špijunaži i izdaji – kojoj se nije nazirao kraj.

Deo II

28.
Ćao, ChaO

Iz svog istraživanja DarkMarketa s Kitom Mularskim, inspektor Šen je znao da ChaO ima i svoj sopstveni sajt: CrimeEnforcers.com (šegačenje na račun fraze „law enforcers",[38] koju je bratija s one strane zakona odavno svela na skraćenicu LE, budući da se u onlajn diskusijama pojavljuje vrlo često).

Na naslovnoj stranici sajta CrimeEnforcers, ChaO je objašnjavao svoje ciljeve i usluge:

> Mi smo privatna organizacija za vaše posebne zahteve za izradu. Naš fokus je na elektronici i kompjuterskom inženjeringu. Ako vam je potreban specijalni hardver (pogotovo hajtek) ili softver koji se u vašoj zemlji ne proizvodi ili čak i ne pominje, iz bilo kog razloga, kao što su zakoni i tako to, na pravom ste mestu.
>
> Nudimo vam apsolutno anoniman & ofšor razvoj vaših projekata. Nije nas briga šta ćete vi da radite sa softverom i hardverom koji tražite da napravimo za vas.
>
> Nije potrebno naglašavati da nam je vaša privatnost veoma važna i da ni iz kog razloga ne otkrivamo nikome ništa. Ne treba nam vaše ime, adresa i tako to. Treba nam samo vaš imejl. Dobićete sertifikat i nalog za bezbedno logovanje na naš privatni forum, da možete da pratite razvoj svoje porudžbine, možete čak i da postavljate pitanja tehničarima koji rade na vašem projektu.
>
> Ako ste došli do ovog sajta, onda već znate za nas. Mi ne radimo za male pare i nećemo da se uortačujemo s vama. Ako želite da vam se snovi ostvare, morate da imate dovoljno

38 Eng.: *law enforcers* – „oni koji sprovode zakon": policajci, agenti kriminalističke službe. Izraz *crime enforcers* ima suprotno značenje, otprilike „oni koji sprovode kriminal", tj. kriminalci, zločinci, prestupnici i sl. (Prim. prev.)

novca da uložite za svoje snove. Morate da platite čak i za procenu koliko će vaš projekat da košta.

Kad se naviknete na njegov pomalo iskvaren i pojednostavljen „globiš", ChaO-v poslovni plan postajao je jasan. Nudio je logističke usluge i podršku svima zainteresovanima za karijeru u sajber kriminalu. Umesto da se sâm bavi kriminalnim radnjama, olakšavao je manje veštim korisnicima kompjutera da započnu tu praksu. Kompjuterski kriminal je počeo da podražava poslovne modele iz stvarnog sveta.

Na ostalim stranicama sajta *CrimeEnforcers.com* mogli ste pogledati robu koju je nudio ChaO. Skiming uređaj bio je njegov zaštitni znak i za kratko vreme porudžbine za skimere prerasle su u vrlo uspešan posao.

CrimeEnforcers je nudio i mobilne čitače kreditnih kartica – prenosive uređaje za provlačenje kartica, onakve kakve viđate po restoranima. Početkom 2007. policija je u nekoliko delova Engleske otkrila grupu radnika na bezinskim pumpama koja je kupila veći broj tih uređaja, za koje se veruje da su potekli ili od kanadskog DarkMarketara Drona ili iz ChaO-ve fabrike. Kad bi mušterija pružila kreditnu karticu, radnik na pumpi bi je prvo vešto provukao kroz ilegalni čitač ispod tezge, koji je beležio podatke sa nje, a tek onda kroz legitimni uređaj.

Onima koji su pravili prve nesigurne korake na polju sajber kriminala, CrimeEnforcers je davao gomilu korisnih saveta koji su umnogome olakšavali taj proces. Za apsolutne početnike, sajt je postavljao korisna video-uputstva u kojima je animirani ChaO, blagosloven elektronskim glasom koji je ipak odavao karakterističnu boju i naglasak stvarnog čoveka, nudio savete i napomene o tome kako da odaberete najbolje bankomate kad planirate da izvršite zločin.

Učio je svoju publiku, na primer, da je instaliranje skimera na bankomatima u mestima gde postoji visoka koncentracija ilegalnih imigranata loša zamisao (na tim bankomatima nema mnogo prometa, ali zato ima mnogo radoznalih očiju i previše kokurencije). Umesto toga, predlagao je njihovo postavljanje u blizini noćnih klubova, „gde bogati klinci često koriste kredite kartice svojih roditelja".

Pouzdani dobavljač industrije zločina, ChaO je video da se njegovo ime velikom brzinom raširilo internetom, pa mu je bilo izuzetno važno da učvrsti reputaciju i izbegne otkrivanje.

Podrazumevala se generalna upotreba „globiša",[39] drugog jezika bastardiranog engleskog, koji je postao *lingua franca* Mreže, s ulogom šifre koja je omogućila Brazilcima da komuniciraju s Koreancima i Bugarima da razgovaraju s Indonežanima; uskoro su spelovanje i upotreba reči čak i kod onih kojima je engleski maternji jezik počeli da se na internetu razvijaju u brojnim osobenim pravcima. Možete da nagađate o poreklu autora posta, ali obično nije moguće da iole precizno odredite njegovu ili njenu nacionalnost.

To se ne odnosi na Ruse ili Kineze. Autori postova na kriminalnim sajtovima ruskog govornog područja pune svoje komentare lokalnim žargonom, koji su neki lingvisti možda i u stanju da prate, ali samo će ih oni najtalentovaniji i ponoviti tako da niko ne primeti da im to nije maternji jezik. Agenti FBI-ja neće se nikad odati na forumu na kojem se komunicira na engleskom, ali na ruskom forumu bi imali muke da prođu prvi login. Iako su agenti kriminalističkih službi i obaveštajci iz SAD povremeno koristili usluge onih kojima je maternji jezik ruski ili kineski, svakako nikad nisu posedovali ni izbliza dovoljno finansijskih i lingvističkih resursa da preuzmu kontrolu na ruskom sajtu onako kako su delimično prisvojili DarkMarket.

Na sajtovima engleskog govornog područja, međutim, čovek je mnogo manje siguran u pravi identitet sagovornika. Posredovanje Mreže omogućilo je ljudima da menjaju svoju ličnost, čak ih je podstaklo na to. To ni slučajno nije ograničeno na svet kriminala. Sajtovi namenjeni upoznavanju („online dating") već su bili poprište najmasnijeg laganja u istoriji. U sobama za ćaskanje, ljudi su voleli da ostavljaju utisak talentovanih i važnih osoba, što je retko kad odgovaralo prizemnoj stvarnosti njihovog života. Mreža je to podstrekavala zato što ljudi nikako nisu mogli da provere bihevioralne karakteristike svojih virtualnih partnera.

39 *Globish*, reč skovana od izraza *global English*, tj. „globalni engleski jezik", kojim se mahom sporazumevaju učesnici internet foruma i soba za ćaskanje. Lingvisti smatraju da se u njemu koristi oko 1.500 reči (poređenja radi, *Oksfordski rečnik* sadrži 615.000 reči), a karakterišu ga „stenografsko" pisanje (npr. *u* umesto *you*, *r* umesto *are*, *2* umesto *to* ili *too*, *4* umesto *for* i tome slično), krajnje svedena gramatika i pravopis, kao i masovno korišćenje postojećih i novostvorenih idioma. (Prim. prev.)

Svi su dolazili do zaključka da na Mreži mogu da lažu bez straha od razotkrivanja ili bruke.

Kriminalci su pak ne samo podlegali istim zakonima lažljivosti nego su ih, štaviše, naročito dobro koristili u praksi. DarkMarket je pružio obilje dokaza za to. U razgovorima na forumu je opaki Devilman,[40] na primer, projektovao imidž mladog i razuzdanog švalera (mada su mu najveća ljubav bili i ostali jeftini „dampovi"). Međutim, kad su detektivi pokucali na vrata kuće sa dva stana na broju 62 u Ulici Lajm tri grouv u Donkasteru, gde je stanovao Džon Makhju, Devilmanov alter-ego u stvarnom životu, otvorio im je muškarac na početku sedme decenije života, čija je prva reakcija na vest da je uhapšen glasila: „Samo čas, da stavim veštačke zube." Kad je na suđenju nabrajao okolnosti za koje je smatrao da bi trebalo da mu donesu blažu presudu, između ostalog je pomenuo i to da već ima jedan veštački kuk i da čeka da mu ugrade i drugi, zbog čega mu je pokretljivost krajnje ograničena.

Međutim, ozbiljni sajber kriminalci moraju da generišu poverenje ako hoće da razviju posao: reputacija im je od ključnog značaja. Na DarkMarketu, titulu „dobavljača" mogao si da zaradiš samo ako administratorima i na zadovoljstvo kupaca dokažeš da si u stanju da na tržište izbaciš ukradene kartice koje zaista „rade". Te transakcije je nadgledalo pet administratora (posle JiLsijevog izbacivanja sa sajta i hapšenja Matrixa, samo trojica) – Master Splyntr, Shtirlitz i ChaO (a kasnije se u taj deo posla uključio i Lord Cyric).

ChaO se DarkMarketu pridružio u februaru 2006, ali njegove čudesne sposobnosti su mu osigurale brz uspon kroz hijerarhiju. Kad se učvrstio na položaju kneza DarkMarketa, mogao je da se usredsredi na svoju stvarnu poslovnu strategiju. Želeo je da postane najveći dobavljač skiming aparata i ilegalnih čitača kartica u svetu. Za tim uređajima je vladala velika potražnja i, ako mu uspe da stvori monopol, moći će da pređe na sledeću fazu svog plana za maksimalno povećanje prihoda uz minimalan trud.

Naš čovek iz Istanbula bio je zadužen i za DarkMarketov ključni Garantni servis, što je možda bio centralni položaj u celoj operaciji. Delujući kao pošteni broker, osiguravao je da ni kupac ni prodavac kreditnih kartica i drugih ilegalnih podataka ne oštete jedan drugog. U tom smislu, DarkMarket je bio mafijaška

40 Lik iz istoimenog japanskog horor stripa (mange); *Devilman* u prevodu znači „čovek-đavo". (Prim. prev.)

operacija u originalnom smislu reči. Delovao je kao policajac ili arbitar kriminalnog tržišta, baš kao što su časni ljudi počeli nadzirući zelene pijace na Siciliji u drugoj polovini XIX veka, da bi potom prešli na ilegalnu trgovinu oružjem i građevinskim dozvolama.

ChaO-v ugled neumoljivo poštenog garanta usluga izgrađen je na uspehu koji je postigao kao veletrgovac skiming uređajima. Svi su mu verovali. On pak nije verovao nikome. Nikad nije odao svoju IP adresu; nikad nije poslao poruku koja bi ga mogla umešati u nezakonitu radnju a da je prethodno nije enkriptovao; i niko ga nije mogao digitalno locirati.

Prihvativši da je ChaO stvorio u sajber svemiru crnu rupu u kojoj je bio bezbedan i nevidljiv za policiju, Bilal Šen je zaključio da će, ako hoće da uđe u trag svom osumnjičenom, morati da se osloni na tradicionalnije metode policijskog rada – faktor „pešačenja" se ispostavio kao iznenađujuće važan u radu sajber policajaca.

29.
Nežno nežno nežnije

Istanbul, Turska, 2008.

Mada se još pribojavao da ChaO možda uživa zaštitu odozgo, Bilal Šen je svejedno terao dalje sa svojom istragom. Agentu Mularskom obećao je da će po povratku u Istanbul ostati u bliskom kontaktu s njim. Razgovarali su o mogućnosti da zatraže usluge ChaO-vog garantnog servisa na DarkMarketu, da vide mogu li ga tako isterati na otvoreno, ali su brzo zaključili da je to previše komplikovano i da je malo verovatno da će uroditi plodom.

Drugo što su o njemu znali bilo je, dabome, da trguje skimerima. Nije mu bilo moguće ući u trag digitalnim putem. Ali ako ChaO prodaje te aparate, rezonovao je Bilal, tada njegova operacija ima dve slabe tačke – njihovu proizvodnju i otpremanje.

Skiming bankomata postao je tako popularan sport u Turskoj, da je sada sve više policajaca učilo kako da ih uoči nakon što su postavljeni. Mnogi uređaji bili su delo amatera, loše napravljeni i nestručno ugrađeni. Međutim, prelistavajući izveštaje o hapšenju i konfiskaciji, inspektor je primetio da se njihov dizajn i stil u nekim oblastima ne samo poboljšava nego i da izgleda da se proizvode u velikim količinama. Negde mora da postoji fabrika. Obaveštajci su skrenuli Šenu pažnju na moguće prisustvo fabrika skimera u Rumuniji i Bugarskoj, stoga je policijama tih zemalja poslao dopise s molbom za pomoć. Druga mogućnost bila je da ChaO svoju operaciju vodi preko tobože legitimnog biznisa, a čitače kartica nabavlja od ovlašćenih proizvođača u Turskoj.

Pošto nabavi skimere, ChaO mora da ih nekako distribuira. Mularski i Šen su pronašli neke dokaze koji su nagoveštavali da njegovi proizvodi putuju čak do Sjedinjenih Država, Novog Zelanda i Južne Amerike, te da deo pošiljki otpada na porudžbine na

veliko. U tom slučaju, nije bilo verovatno da ChaO koristi kurire. S obzirom na količine koje je počinjao da otprema, to je po svoj prilici bilo obeshrabrujuće komplikovano. Bilal je razmišljao o razlozima za povećanje produktivnosti, ali to razmišljanje nije dalo rezultata.

Nije znao da se ChaO pre godinu dana, krajem proleća 2007, posvađao sa Dronom, kanadskim stručnjakom za skimere koga su se Tajna služba i detektiv Spenser Frizel iz policije Kalgarija spremali da uhapse. ChaO je tvrdio da je Dron „težak tip" koji nervira svoje mušterije i tako blati dobro ime DarkMarketa. Brojne pozitivne poruke o Dronovim uslugama nagoveštavale su pak da je ChaO možda imao sasvim drugačije motive – svakako su ostali karderi na forumu tvrdili da se na Drona nameračio promišljeno, iz svojih razloga.

Nekih mesec dana pre no što je detektiv Frizel uhapsio mladog kanadskog graditelja i prodavca skimera, ChaO je, koristeći svoj položaj administratora, objavio da će Dron biti isključen sa DarkMarketa bez dozvole da se vrati. Sada je mogao da stavi u dejstvo svoj plan da zagospodari tržištem skimera i krene u akciju.

DarkMarket je obezbeđivao vitalno važnu platformu za Dronovu robu – veliki broj njegovih uređaja kupovali su karderi koji su na forumu videli njegov plaćeni oglas. DarkMarket je korišćen i kao primarni oglašivač sajta *CrimeEnforcers.com*, putem kojeg je ChaO prodavao svoje skimere. Pored skimera, ChaO je sajber kriminalcima-poletarcima nudio pakete rešenja, koji su obuhvatali obuku, uputstva i svu opremu potrebnu za start-ap operaciju.

Međutim, čim je uklonio Drona iz jednačine, promenio je svoj poslovni model: zainteresovane strane više nisu mogle da kupe njegove skimere; umesto toga, mogle su da ih iznajme. ChaO im ih je i dalje slao, ali uz malu dodatnu modifikaciju.

Posle Dronovog izbacivanja, ChaO je bio u položaju da podigne cenu svojih skimera – sada su mogli da se iznajme za 7.000 dolara, umesto da se kupe za 5.000. Za taj novac, klijenti su dobijali sa skimerom i PIN podmetač. Kad klijent banke ubaci karticu i ukuca svoj PIN, sve se beležilo na lažnom podmetaču i na skimeru. Potom su se dve prevarantske naprave uklanjale i ChaO-v klijent je pomoću USB kabla daunloudovao informaciju na kompjuter.

S Dronovim skimerima, klijent je mogao da upotrebi tu informaciju da se nezakonito domogne novca. Međutim, sa ChaO-vim

skimerima, podaci koji su se učitavali u kompjuter bili su enkriptovani. Jedini koji je posedovao ključ za njihovo dekriptovanje bio je... ChaO. Stoga kriminalac-poletarac koji se toliko namučio da postavi skimer i PIN podmetač u bankomat nije mogao prosto da izađe i sam klonira karticu – morao je da pošalje informaciju natrag u Istanbul. ChaO bi potom organizovao unovčavanje. Kad dobije novac, slao je klijentu – koji je zapravo obavio onaj teški deo posla – njegov deo. Zapravo je svoje skimere rentirao – što je bila mnogo profitabilnija strategija od Dronovog prodavanja uređaja.

U svetu sajber kriminala, bio je to odvažni novi poslovni model. Da je uspeo, ChaO bi sigurno zaradio neiskazane sume novca, ubirući „kajmak" u vidu ogromnog procenta od ilegalnih skimerskih transakcija širom sveta. Morao je samo da obnavlja svoju zalihu skimera i otprema ih a da ga pri tom ne uhvate. Što nije prevazilazilo njegovu snalažljivost. Naravno, postojala je mogućnost da će neki konkurent u izvesnom trenutku pokušati da ga pobedi jeftinijom ponudom ili, prosto, povratkom na raniju običnu prodaju skimera. Dotle je, međutim, budući da je vladao na najuticajnijem forumu na engleskom govornom području, ChaO mogao da uživa u životu na visokoj nozi. Bogme je i uživao.

Godine 2008. Istanbul je uveliko bio na putu da postane grad s najvišom stopom razvoja u svetu. Populacija je poslednjih petnaest godina narastala gotovo nekontrolisano i sada je brojala petnaestak miliona stanovnika, od kojih je, prema procenama, bilo oko dva miliona neprijavljenih imigranata, ne samo stranaca nego i anadolskih Turaka i Kurda što su se slivali u grad na obalama veličanstvenog Bosfora, te velike vode što razdvaja Evropu i Aziju.

Za razliku od mnogih gradova u Istočnoj Aziji, pogotovo u Kini, taj fenomenalni i energični razvoj Istanbula nije išao nauštrb njegove blještave baštine – istorija tu nastanjuje skoro svaku građevinu. Posvuda je vidljiva bogata tradicija više od jednog milenijuma duge vizantijske prošlosti i šest stotina godina osmanlijske raskoši – dvaju najmagičnijih, najnasilnijih, najuspešnijih i najimpresivnijih imperijalnih tvorevina svih vremena. Nasuprot opštoj maštovitoj zamisli, Osmanlijsko carstvo je za vreme najvećeg dela svog postojanja bilo poznato po tolerantnosti svojih vladara prema ostalim „sledbenicima Knjige" – Jevrejima i

hrišćanima. Njegova nasilnička reputacija potekla je od krvavih pokolja u dalekoj prošlosti, da bi se ponovo ispoljila za vreme spore propasti ove imperije u XIX i početkom XX veka.

U turskoj republici koja se posle Prvog svetskog rata podigla iz pepela Carstva, Istanbul je prošao kroz neka krizna razdoblja: prvo onda kad je izgubio status prestonice u korist Ankare, zabačenog gradića u Anadoliji;[41] i kasnije, za vreme Hladnog rata, kad je nemilosrdna vojska nastojala da uguši nezavisni duh grada. Njegova infrastruktura počela je da se urušava i narod je počeo da se iseljava, pa je populacija dugo stagnirala na oko dva miliona. Međutim, Istanbul je negde od početka devedesetih godina prošlog veka grabio krupnim koracima i povratio sebi mesto među najdinamičnijim i najintrigantnijim gradovima sveta.

Mnogoljudan, bučan i sav nabujao od života, s ekonomskom aktivnošću koja neprestano leti tamo-amo između njegovog evropskog i azijskog dela, Istanbul je ponekad umeo da utera čoveku u kosti osećaj klaustrofobije onim desetinama hiljada rasklimatanih automobila i kamiona što su svakodnevno prelazile preko dva kontinentalna mosta. Saobraćaj se na evropskoj strani puževim korakom vukao oko Trga Taksim ili duž kule Dolmabahče i nekadašnjih carskih vrtova što gledaju preko u Aziju. Čak i kad je bilo prohladno, prašina se i dalje zavlačila u gušu. Međutim, poslednjih desetak godina grad prosto cepti od mogućnosti – umetničkih, komercijalnih i političkih – i malo je većih zadovoljstava u životu nego kad se posle dugog radnog dana voziš trajektom iz Evrope, posmatraš Bosfor i spremaš za dobru večeru u Kadikoju, na azijskoj strani.

I pored svih strahova da je vladajuća AKP možda peta kolona islamskog fundamentalizma, otkako je ona na vlasti, istanbulska mlada srednja klasa zgrabila je obema rukama pruženu ekonomsku priliku i počela da stvara uspešne proizvodne, dizajnerske, haj-tek i uslužne kompanije ravne najboljima u Evropi, Americi i Aziji.

Razume se, održavanje zakona u gradu je prava noćna mora, pogotovo zbog toga što vrlo malo njegovih žitelja gaji ikakvo poverenje u snage koje su decenijama bile ključni simbol represivnog državnog aparata.

41 U vreme preseljenja vlade u Ankaru, to je bila varoš od jedva tridesetak hiljada duša. Istanbul je sa svojih pola miliona stanovnika bio velegrad u odnosu na nju; pa i danas je Ankara više nego tri puta manja od njega (ima populaciju od nešto manje od 4,5 miliona). (Prim. prev.)

Novi zločini urodili su novom vrstom policajca, a Bilal nije imao nikakve veze ni sa kakvim starim tradicijama Države u državi, niti je stvorio sebi neprijatelje od nekih posebno moćnih ljudi, pa su ga dočekali s dobrodošlicom kad je došao iz glavnog grada, Ankare, s ciljem da otkrije distributivnu mrežu skiming operacije koju je vodio ChaO.

Međutim, ipak govorimo o Istanbulu; inspektor Šen je tragao za iglom u plastu sena. Legalan, polulegalan i nelegalan izvoz i uvoz vekovima je bio zaštitni znak gradske privrede – otpremanje i dopremanje najrazličitije robe. Od šezdesetih godina prošlog veka, ogromne količine bele tehnike našle su put do Istanbula, preko Balkana, iz Nemačke, gde je emigriralo oko dva miliona Turaka da bi tamo bili gastarbajteri. Međutim, od pada Sovjetskog Saveza, razmere ove trgovine probile su sve granice: otvorila su se nova tržišta u Rusiji, Ukrajini, Kavkazu i u više centralnoazijskih republika u kojima se govori turkijskim jezicima.

Bilal je, međutim, odnekud morao da počne, pa je odabrao tri najveće transportne kompanije u gradu. Pre toga su on i njegov pomoćnik pola dana proveli obučavajući osoblje kurirskih firmi kako da uoče skimer. Ti uređaji, naime, najčešće imaju deklaraciju na kojoj su registrovani kao rezervni delovi za vozila ili mašinske alate. Zatim su im dali skimere u ruke, da se naviknu na njihovu težinu i oblik.

Nizali su se dani koji nisu davali rezultata i inspektor Šen je zaključio da bi trebalo da se vrati u štab jedinice u Ankari. Posle nekoliko nedelja, počela je da ga hvata dobro poznata potištenost. A onda, posle samo mesec dana, iz Istanbula je stigla dobra vest – u jednu od onih transportnih firmi došao je čovek s paketom adresiranim na Finsku. Ispostavilo se da je to skimer. Šalterski radnik pozvao ga je iz sporedne prostorije i javio mu da se u paketu nalazi i PIN podmetač.

„Bingo!", pomislio je Bilal, rekavši šalterskom radniku da pusti pošiljaoca da ide: već su ga bili snimili putem kamera interne televizije. Posle mnogo meseci, inspektor je konačno naišao na trag. Nimalo iznenađujuće, onaj čovek je upotrebio lažnu ličnu kartu, ali onda je usledio još jedan prelomni momenat. Osumnjičeni je dao kurirskoj firmi i tri telefonska broja – od kojih je jedan bio stvaran. Proverili su ime kako bi utvrdili zakonitog vlasnika telefona: nije se činilo da pripada kriminalcu. Međutim,

pratili su mobilni broj, a čovek koji je doneo paket ga je koristio – telefon je bio aktivan.

„Ovaj će nas možda dovesti do ChaO-a", pomislio je Bilal.

Ali našao se suočen sa dilemom. Otprilike baš u to vreme *Haber 7* objavio je fotografiju poniženog hakera Merta Ortača, pa je pritisak na istanbulsku policiju, koja je bila zadužena da nađe Ortača, i na Bilala, čija je primarna meta bio ChaO, bivao sve veći. Bilal je morao da ubrza istragu, ali znao je da ne sme dozvoliti da nestrpljenje ugrozi operaciju.

Otmicom Ortača, ChaO je prvi put odao strah i slabost. Ali zašto ga je ono što je Ortač otkrio *Haberu 7* toliko uznemirilo?

ChaO je znao da je Ortač Turčin. Isto tako, izgledalo je da veruje da je ovaj policijski doušnik. Štaviše, shvatio je da je Ortač u bekstvu i da je uplašen. Rizik da će progovoriti ako ga se policija prva dokopa bio je vrlo stvaran.

Ali ko je, kog đavola, bio Mert Ortač i kako se našao upetljan u ovu neverovatnu kriminalnu aferu? Sve je počelo prethodnog proleća, pripremanjem hapšenja Matrixa i JiLsija – o čemu Ortač, naravno, nije ništa znao – koje je označilo kraj prve faze u Operaciji DarkMarket i početak druge faze.

Deo III

Orijentacija

Za samo godinu dana, DarkMarket me je odveo daleko, od sedišta Googlea do restorana u Čihangiru, pomodnoj četvrti neposredno ispod Trga Taksim u evropskom delu Istanbula. Preko puta mene poigravao je vedar osmeh Merta Ortača. Nakon što sam proveo nekoliko sati u njegovom društvu, zaključio sam da pridev „nestašan" otkako je sveta i veka nije nikome pristajao tako dobro kao Mertu.

Za vreme jedne opuštene večere u Kadikoju, moj prijatelj Šebnem i ja držali smo svoje ajfone na stolu. Najednom su nas istovremeno upozorili da smo dobili SMS poruku. Ona koju sam ja dobio bila je poslata sa Šebnemovog telefona, a Šebnemova s mog. Obe su glasile: „Pozdrav od Merta!" Dok smo ih čitali, s drugog kraja stola dopro je Mertov veseli smeh, zajedno s objašnjenjem da je uspešno hakovao međunarodni roming sistem. Kao rezultat, nastavio je, mogao je da pošalje poruku s bilo kog mobilnog telefona na svetu na bilo koji drugi – u pogrešnim rukama (kao što su Mertove), takvo umeće može da pretvori život u beskrajni niz šekspirovskih zapleta zasnovanih na nesporazumima, i tragičnim i komičnim.

Dopisivao sam se s Mertom dok je bio u zatvoru, odakle mi je poslao deliće priče koja je samom svojom domišljatošću nadmašila sve ostale legende DarkMarketa. I dok sam, razgovarajući s većinom ostalih likova umešanih u DarkMarket, bio svestan da mnogo toga prećutkuju, Mert je samo sipao informacije, anegdote i priče od kojih se čoveku vrtelo u glavi.

Od ključne je važnosti da hakeri, sajber kriminalci i sajber policajci u potpunosti vladaju svojim podeljenim životom – moraju da znaju gde je granica između stvarnog i virtualnog, i moraju biti kadri da se isključuju prilikom prelaska iz jednog svog života u drugi. Mert u svojoj glavi uopšte nije umeo da odredi kada govori istinu a kada ne.

Život bi bio neuporedivo lakši da je Mert bio bestidni maštar koji je prosto pričao gluposti. Ulaženje u trag hakerima, članovima i policajcima povezanim sa DarkMarketom izvesno je bilo

jedno od iskustava koja su me u mojoj novinarskoj karijeri najviše iscrpela. Međutim, ništa nije bilo toliko razdražujuće kao pokušaj da utvrdim verodostojnost Mertove priče. Zapravo, to nije sasvim tačno: ispostavilo se da je najveći deo onoga što je ispričao tačan i u suštini autentičan, ali mestimično u toj meri nakićen da se preobrazio u nešto sasvim drugačije. Čudno je, ali najveće Mertove laži odnosile su se često na krajnje prizemne stvari, koje je bilo najlakše proveriti. Na primer, mrtav hladan mi je rekao da je rođen 10. aprila 1982, dok se u stvari jeste rodio tog dana, ali četiri godine kasnije.

U poglavljima koja slede, kazujem Mertovu priču umnogome onako kako ju je on meni ispričao. Međutim, postoje dva ključna trenutka kad njegova pripovest jednostavno nema smisla i ne mogu da utvrdim tačnost tih tvrdnji; štaviše, u prvom slučaju, jedan od glavnih likova glatko poriče Mertovu verziju događaja. Upozoriću čitaoca kad stignemo do tih trenutaka.

Konačni test Mertovog kredibiliteta leži u njegovom odgovoru na pitanje koje još od nastanka DarkMarketa muči mnoge verne sledbenike sajber podzemlja. Ko je bio Lord Cyric?

30.
Svet mašte Merta Ortača

Istanbul, Turska, maj 2007.

Kad su ga uveli u salon raskošne vile, Mertu Ortaču je zastao dah. Prostorija ga je podsetila na Sultanov apartman u Palati Čiragan, remek-delu s kraja XIXveka, sagrađenoj na zapovest njegovog carskog visočanstva sultana Abdul Aziza, koja se odnedavno nalazi u posedu hotelskog lanca Kempinski. Sofe i fotelje imale su pozlaćene ukrase, dok su zidne tapete sa arapskim šarama svetlucale na suncu.

U stvari, Palata Čiragan dizala se samo 800 metara daleko od vile, koja se pak nalazila izolovana na strogo čuvanom imanju. Posvuda oko njega krstarili su agenti i mrštili se na sve koji su se drznuli da pokušaju da parkiraju auto u blizini. Smeštena na samom obodu istanbulske opštine Bešiktaš, vila je s vrha evropskog brežuljka gordo gledala preko Bosforskog moreuza u Aziju. Više od svega bilo je iznenađujuće to što se salon u koji su uveli Merta nije dičio portretom Kemala Ataturka, poštovanog osnivača moderne Turske. Kemalovi portreti su u Turskoj obavezni, i to ne samo u privatnim i javnim poslovnim prostorima: neretko ćete ih naći u svakoj prostoriji u zgradi. Ali ne i u ovoj, uprkos tome što je vila bila deo istanbulskog regionalnog sedišta turske Nacionalne obaveštajne agencije (Milli Istihbarat Teskilati, MIT).

U krajnje uznemirujućim situacijama, Mert je reagovao tako što se blago kikotao iza svog zarazno nestašnog osmeha, ili bi presekao i zbrisao. Ovo je bila prilika u kojoj nijedan od ta dva postupka nije bio primeren. Mert je bio prosto hipnotisan prizorom elegantnih konobara koji su ih poslužili čajem i kafom. Pogotovo su mu se u pamet urezale njihove besprekorne bele rukavice dok su spuštale zakusku na sto ispred njega. Obuzeo ga je

nestvaran osećaj dobrobiti i prigušenog oduševljenja. Nije, međutim, dugo potrajalo.

Pored njega je bio kolega iz Instituta za tehnologiju, ali Mert nije poznavao ostalu trojicu koja su ga dočekala. Kad su se konobari nečujno povukli, ti ljudi su usmerili pažnju na Merta. „Želimo da ti postavimo nekoliko pitanja", rekao je jedan. Zatim su spustili ispred njega digitalni diktafon.

Nedugo potom već se preznojavao pod pritiskom ispitivanja. Međutim, nisu ga maltretirali. Umesto toga, šest i po sati su od njega tražili da rešava opako teške matematičke probleme. U normalnim okolnostima ne bi ni pokušao da ih reši bez kompjutera. Njegova tri domaćina zahtevala su da upotrebi metodologiju popularnu u kodiranju, koja je podrazumevala razlaganje broja pedeset dva na neparne brojeve. To je bila visoka matematika, a on nije imao ništa sem olovke i papira.

Mladi kompjuterski programer je već pao na prijemnom ispitu za probni rad u Obaveštajnoj agenciji. Prošao je na testovima iz stranog jezika (engleskog) i matematike, ali je zato imao sramno loš rezultat na testu iz turskog jezika. Bez obzira na to, Agencija je i dalje bila fascinirana njegovim kompjuterskim znanjima. Njegovo poznavanje programiranja bilo je istinski čudesno i izvanredni rezultati koje je postigao doprineli su da ga uzmu za honorarnog saradnika.

Godine 2003. Mert je bio pod krivičnom istragom zbog prevare. Mada je imao samo sedamnaest godina, uspeo je da provali kod koji je enkriptovao smart kartice koje je koristila satelitska TV mreža Digiturk. Bila je to unosna veština. Digiturk je, naime, nedugo pre toga otkupio prava na prenose utakmica Super lige, vrlo popularne elitne lige turskog fudbala. Kako bi dekriptovali kanal, pretplatnici su morali da kupe od Digiturka smart karticu i ubace je u satelitski risiver, koji ih je potom propuštao u fudbalski raj.

Čim je shvatio kako da provali ove kartice, Mert je počeo da ih reprodukuje za ilegalnu prodaju na ulicama Istanbula, što mu je obezbeđivalo dobru zaradu. Međutim, kako mu se jedan džep punio turskim lirama, tako ih je on iz drugog džepa vadio. Mert je priređivao žurke za prijatelje koje je pozivao iz Ankare i plaćao im put i smeštaj po dolasku u Istanbul. Nikad nije umeo da kontroliše svoje trošenje, čak ni kasnije, kad mu je karding donosio velike sume novca.

Mertu su njegovi prijatelji bili veoma važni, delom i zato što je ponekad bio željan pažnje i naklonosti. Da li je bio svestan toga ili ne, tek, novac zarađen od Digiturka koristio je da kupuje prijateljstvo – a Istanbul je bio pun dvadesetogodišnjaka spremnih da se druže s mladićem koji je očigledno bio voljan da finansira skupe zabave. Naravno, kad god bi ponestalo novca, većina tih likova bi netragom nestala.

Takođe, Mert je očajnički želeo da dokaže kako je nešto posebno (što je, s obzirom na svoj kompjuterski talenat, nesumnjivo i bio). Stoga je sistematski preuveličavao svoja dostignuća. S razvojem te tendencije, Mertova svest počela je trajno da lebdi negde između stvarnosti i mašte. Čini se da je vrlo rano izgubio sposobnost da ih razlikuje. Bili su tako beznadežno prepleteni da bi detektor laži, da su ga ikad prikačili na njega, po svoj prilici sasvim poludeo ili ne bi registrovao baš ništa. To je, razume se, s jedne strane značilo da se s lakoćom prilagodio kulturi interneta – toj dolini laži.

Posle niza IT poslova u raznim kompanijama, Merta su u junu 2006. primili u lokalnu filijalu Tošibe, čijem je kadrovskom odeljenju nekako promaklo da se on nalazi pod istragom zbog Digiturk prevare. Bez obzira na to, kolege u Tošibi su vrlo brzo počele da se čude njegovom ponašanju. Takođe su bile malčice sumnjičave u vezi sa sertifikatom koji je, navodno, potvrđivao da je diplomirao kriptologiju na Univerzitetu u Kembridžu.

Upravni odbor, pisalo je na sertifikatu, „daje mu ovu diplomu kao dokaz izdat u tu svrhu u Londonu, u Kembridžu, dvadeset drugog dana meseca juna dve hiljade četvrte".

Možda su mu diplomu dali u londonskom pabu *Kembridž arms*? Gde god da se odigrala ta izmišljena ceremonija, sertifikat je bio tako primitivno napravljen da je teško zasluživao da se nazove falsifikatom.

Jednom njegovom kolegi u Tošibinom IT odeljenju upalo je oči Mertovo često razmetanje vezom s Nacionalnom obaveštajnom agencijom. I sâm im je povremeno pomagao, pogotovo potkraj devedesetih, kad je Agencija tek trebalo da razvije sopstveni efikasni sajber odsek. Međutim, to nije bilo nešto čime se čovek hvališe. Mertovo neprestano brbljanje kako je blisko povezan s obaveštajnom službom stvarno je išlo na živce. Ipak, Tošiba ga je držala šest meseci jer je obavezno nalazio rešenje za svaki

problem koji bi šefovi zatražili da reši. Shvatili su da je pametan, ali nešto im je govorilo da pažljivo motre na njega.

Uveče su Merta pozivali u Obaveštajnu agenciju i tražili od njega forenzičke procene raznoraznih hard diskova i kompjutera koji kao da su padali s neba. On je pak trebalo da iskopa fajlove, provali lozinke gde god je moguće i isporuči im sav eventualni inkriminišući materijal. Unutrašnja bezbednost Turske bila je primarna odgovornost Agencije, zbog čega je njen zadatak bio da motri na brojne organizacije za koje je vlada smatrala da su umešane u terorizam.

Negde pred kraj 2006. Tošiba je otpustila Merta – nije se ponašao kako valja, nekako se previše hvalio svojim sumnjivim podvizima s kreditnim karticama, a opet, istovremeno je neprestano tražio od kolega novac na zajam ili isplate bonusa.

Mert je tvrdio da je iz Tošibe otišao po nalogu svojih šefova u Nacionalnoj obaveštajnoj agenciji, koji su, rekao je, već radili na tome da mu nađu drugo radno mesto kojim će prikrivati svoj pravi posao.

Neposredno pre no što je počeo da radi na novom radnom mestu, njegov instruktor mu je doneo hard disk, deo vrlo osetljive istrage. Šefovi su želeli da saznaju sve o svakom fajlu na tom disku, bilo da je vidljiv ili sakriven, dostupan ili enkriptovan. Disk je pripadao jednom od starešina ilegalne levičarske organizacije poznate po akronimu DHKP/C (Devrimci Halk Kurtulus Partisi/Cephesi, odnosno Revolucionarna narodnooslobodilačka partija/front).

Devedesetih i početkom dvehiljaditih, DHKP/C je bila jedna od najnasilnijih i najefikasnijih turskih levičarskih organizacija posvećenih oružanoj borbi. Revolucionarna narodnooslobodilačka partija/front (Partija je bila političko, a Front, u teoriji, militarističko krilo) bila je frakcija Dev Yola, šireg revolucionarnog pokreta, koji je sedamdesetih i osamdeset godina prošlog veka podneo teret vojne represije.

Ta grupa nije bila nikakva drugorazredna ekipa sklepana s koca i konopca – politiku i terorizam shvatali su vrlo ozbiljno, koncentrišući se pre svega da napadaju saradnju između onoga što su proglašavali imperijalizmom NATO-a i turskog vojnog establišmenta. Vršili su uspešne atentate na turske, američke i britanske građane koji su bili uspešni poslovni ljudi ili povezani s vojskom. Za razliku od većine levičarskih naoružanih grupa, ova se

dičila sofisticiranom kontraobaveštajnom delatnošću i, kao takva, bila je trn u oku Nacionalnoj obaveštajnoj agenciji.

Prilikom jedne racije, agenti su došli do laptopa i doneli su ga Mertu u istu onu vilu u kojoj su prvi put razgovarali s njim i u kojoj je sad uvek radio. Njegov instruktor mu je objasnio da je korisnik laptopa pristupao sajtu pod nazivom DarkMarket. Instruktor je i sam bio gik i rekao je Mertu da je pratio veze DarkMarketa sve do servera u Singapuru, koji mu je ličio na proksi. Posle toga, rekao je, digitalni trag se gubio. Nije znao ništa o tome ko stoji iza tog sajta, mada su dokazi snažno ukazivali da je DHKP/C umešana u karding, kojim povećava svoje prihode, a možda ujedno i istražuje upotrebu botneta i mogućnost da joj oni pomognu u ostvarenju njenih ciljeva.

DarkMarket odjednom više nije bio samo kriminalni sajt: sad je i pomagao u finansiranju terorističke organizacije.

Instruktor je upitao Merta zna li išta o tom sajtu.

Mert nije znao. Takođe je uspeo da isprati server DarkMarketa do Singapura, ali dalje od toga nije uspeo da prodre, koliko god se trudio. Za to je bio zaslužan izvanredan posao koji je obavljao Grendel. Bez obzira na to, Mert je rekao instruktoru kako zna nekog ko možda bolje poznaje DarkMarket.

Mert je bio umoran. Nacionalna obaveštajna agencija je od njega očekivala da zadatke koje mu je davala obavi preko noći. Njegovo novo radno mesto bilo je na turskoj TV Fox. Fox Turska nije bio u celosti vlasništvo Ruperta Mardoka i njegove kompanije News International, zato što je turski zakon nalagao da se 51 procenat vlasništva mora nalaziti u rukama turskog državljanina. Ovaj većinski vlasnik bio je nekadašnji diplomata, poznat po svojim vezama u policiji i tajnoj službi. Mertove kolege u Foxu primećivale su da je ovaj često, ako ne i uvek rasejan, kao i da mu je teško da završi čak i jednostavne poslove – ne zato što nije u stanju nego zato što razmišlja o sasvim drugim stvarima.

Jedan od Mertovih kontakata zamolio je mladića da drži na oku izvesnog Saduna Ozkaju, tinejdžera iz srednje klase čiji su se roditelji pribojavali da je zastranio. Upravo su ga bili izvukli iz zatvora, gde se nalazio pod istragom zbog prevare. Kontakt je zamolio Merta da se postara da Sadun ne zaluta ponovo s one strane zakona – kao da je zatražio od jednog vuka da propoveda drugom o blagodatima veganske ishrane dok se obojica oblizuju nad ostacima sočnog jagnjeta.

Mert se razumeo u kriptografiju i programiranje; Sadun se razumeo u kreditne kartice. Vrlo brzo su udružili snage. Na Mertovo zaprepašćenje, Sadun mu je rekao da je član DarkMarketa, na kom koristi dva nadimka, Cryptos i PilotM. U roku od nekoliko sati, Mert Ortač ulogovao se pod potonjim.

O, čuda!, pomislio je Mert dok je prvi put krstario po unutrašnjosti DarkMarketa:

> Kol'ko je mnogo krasnih bića ovde!
> Kako je lep taj ljudski rod! O, divni novi svete,
> Koji imaš baš takve ljude![42]

Mert je bio opčinjen. Istraživao je svaki delić sajta, razgledao forume, naučio da podražava njegov tajni žargon i potom pokušao da na malo zaobilazniji način otkrije njegove tajne. Sve dotad, Mertove kriminalne težnje nisu išle dalje od dekripcije smart kartica i prodavanja kloniranih kartica nakon što im provali kod. Pušten s lanca na DarkMarketu, brzo je skupljao nova znanja o prevarama s kreditnim karticama. Kombinacija tih veština odvešće njega i Saduna u neke vrlo mutne mada novcem bogate vode.

Pre toga, međutim, počeo je da mapira sve u vezi s DarkMarketom, kao da je to neki podzemni lavirint sa skrivenim zamkama i blagom. Njegovi šefovi u Obaveštajnoj agenciji su, naravno, želeli da pronađe sve što može o DHKP/C, terorističkoj organizaciji koju su istraživali. Merta je, međutim, više interesovalo sve ostalo što se događalo na forumima.

Vrlo brzo je shvatio da su ključni članovi sajta ChaO, Master Splyntr, Shtirlitz i Lord Cyric. Naime, kad je Mert počeo da se igra na DarkMarketu, JiLsi i MatrixOO1 su već bili uhapšeni.

Bilo mu je potrebno svega nekoliko sekundi da shvati da je ChaO Turčin, iako se to desilo sasvim slučajno i nije imalo nikakve veze s njegovim hakerskim umećem. Razgledao je oglase za ChaO-ve skiming uređaje, kad je u pozadini ugledao turski znak za doner kebab.[43] Na drugoj fotografiji je skimer namenjen prodaji stajao pored nekog turskog praška za veš.

Vest o velikom turskom uticaju na sajtu preneo je svom šefu, koji se tada još više zainteresovao za DarkMarket: ne samo da

42 Vilijam Šekspir, *Bura*, čin V, scena I (prevod Simić i Pandurović). (Prim. prev.)

43 Nama je poznatiji kao grčki giros (*gyro*). (Prim. prev.)

su levičarski teroristi aktivni na tom sajtu nego još i Turci upravljaju njime! To je moglo biti veoma važno, stoga je zahtevalo dalju istragu. Mert je dobio ovlašćenje da stupi u kontakt sa ChaO-m i svim ostalim Turcima koje eventualno pronađe cunjajući po forumu DarkMarketa. Nije prošlo dugo a pomislio je kako je identifikovao još jednog – Lorda Cyrica.

Mert je počeo da pretražuje arhive s početka devedesetih, kad su mnogi gikovi koristili nešto zvano BBS, Bulletin Board Service („oglasna tabla"), most između elektronskog mesidžing sistema i interneta. Čitajući zapise, zinuo je kad je naišao na dva poznata nadimka jedan pored drugog: ChaO i Lord Cyric! Izgleda, logično je zaključio, da se ta dva glavna mozga DarkMarketa već odavno poznaju.

31.
Sluga dvaju gospodara

Fiktivni Lord Cyric postao je popularan među gejmerima tokom osamdesetih i početkom devedesetih godina prošlog veka. To je bilo samoproklamovano božanstvo koje je proganjalo *Forgotten Realms*, samotni fantazijski svet po kom su ratnici krstarili u potrazi za blagom i mračnim tajnama, usput ubijajući čudovišta s magičnim moćima i destruktivnim porivima. *Realms* su postali omiljena teritorija gejmera, koji su je istraživali preuzimajući fantazijsku ulogu u timu avanturista koji su igrali *Lagume i zmajeve* (*Dungeons and Dragons, D&D*). Te Pustare subtolkinskog sveta pojavile su se docnije u mnoštvu kompjuterskih igrica, između ostalih i u neverovatno popularnoj *Baldur's Gate*.

Opisani su i u mnogim knjigama koje su bile u jednakoj meri nadahnute *Lagumima i zmajevima* i *Gospodarem prstenova*. Lik Lorda Cyrica igrao je ključnu ulogu u mitologiji igrice *Forgotten Realms* – pored toga što je bio bog, bio je i zao do koske. Još važnije za svet kardinga i DarkMarketa, Cyric je *inter alia*[44] bio poznat kao Gospodar laži (Prince of Lies), čije su satanske moći obuhvatale majstorstvo prevare i obmane, kao i sposobnost da podstiče sukobe i spletke.

Ko god da se krio iza tog avatara na CardersMarketu, DarkMarketu i drugde, želeo je da projektuje koncept onoga što gejmeri *Laguma i zmajeva* nazivaju „haotičnim zlom" („chaotic evil"), čime se nagoveštava da taj lik seje haos i beznađe gde god da se zatekne. To je svakako pristajalo Lordu Cyricu sa DarkMarketa kao saliveno, baš kao i njegova sklonost ka prevari i obmani, sukobima i spletkama. Malo je kardera izazivalo toliko neprijateljstva u zajednici kao taj lik. Specijalnost mu je bila da se nabacuje optužbama kroz glasine i aluzije.

Iz razloga koji nikad nikom nisu bili jasni, Cyric bi odabrao metu; jednom je to bio RedBrigade, koji je onako unosno iskoristio Shadowcrew u Njujorku. Potom se dao na posao da mu sa

44 Lat.: *između ostalog*. (Prim. prev.)

hiljadu sitnih pakosti uništi ugled među kolegama karderima. Mali nagoveštaj ovde ili insinuacija tamo da RedBrigade nije ono što izgleda, ili prikrivenih aluzija koje su između redova sugerisale da RedBrigade zapravo radi za snage reda i zakona. Jezik mu je bio sarkastično uvredljiv i nezreo, a opet, pažljivo osmišljen tako da metu njegovih napada maksimalno iznervira i zaboli.

Ipak, Cyric je imao i svoje zaštitnike – a nijedan nije bio tako postojan kao ChaO. S viškom mozga i odgovarajućim kompleksom više vrednosti, ChaO je kao sebi ravne priznavao samo dvojicu korisnika kompjutera. Gajio je beskrajan prezir prema sajber odseku FBI-ja, ali je zato skidao kapu hakerskom umeću Maksa Vižna, poznatog kao Iceman, iako su se njih dvojica zbog Icemanovih napada na DarkMarket često svađali. Kad je pak govorio o Lordu Cyricu, ChaO je išao gotovo toliko daleko da je svom starom prijatelju priznavao kako u hakerskom panteonu zauzima još uzvišeniji položaj od njega samog.

Lord Cyric je za kratko vreme uspeo da se nametne kao glavni moderator i administrator na forumima kao što su The Grifters, CardersMarket i, naposletku, DarkMarket. Nikome nije bilo jasno koju igru igra niti šta pokušava da postigne, mada su oni na koje bi se nameračio smesta pretpostavljali da radi za policiju, bilo kao njen pripadnik ili kao tajni doušnik.

U Pitsburgu, agent FBI-ja Kit Mularski nije imao pojma. Poput mnogih drugih, verovao je da osoba koja se krije iza Lorda Cyrica živi u Montrealu, u Kanadi, ali raspitivanja u sajber odseku Kraljevske kanadske konjičke policije (Royal Canadian Mounted Police, RCMP) nisu donela zadovoljavajući rezultat. Štaviše, mada su se Cyricove IP adrese mogle pratiti do Montreala, povremeno bi se pojavile kao da se nalaze u Torontu, i neki detektivi su podozrevali da zapravo tamo i živi.

Više kardera je poverovalo glasinama da je Lord Cyric u stvarnosti Brajan Krebs, novinar koji piše o sajber bezbednosti, a koji je u to vreme radio za *Vašington post*. Za to nije bilo nikakvih dokaza – štaviše, sve govori sasvim suprotno, jer je Krebs previše ozbiljan pisac da bi rizikovao da uništi sebi ugled petljajući se s ljudima koje istražuje. Pričalo se svašta, ali nikad niko nije uspeo da dokuči ko je zaista Lord Cyric ili čime se bavi.

Premda je ostale nagovarao da se bave svim mogućim sumnjivim radnjama, sâm Lord Cyric nikad se nije upustio ni u kakve

nezakonite transakcije, što potkrepljuje tezuj da je radio za neku kriminalističku službu ili obaveštajnu agenciju.

Svi su, međutim, bili ubeđeni da odlično poznaje karding zajednicu i njeno funkcionisanje. Baš zato je bio toliko tražen. Karderi su hteli da ih poveže s ljudima za koje može da garantuje, a neki su želeli i da saznaju šta zna o njima samima. A policija u SAD i Zapadnoj Evropi još traga za njim u nadi da će ga nagovoriti da im se pridruži u njihovom krstaškom pohodu protiv sajber kriminala.

Cyric je bio suštinska figura sajber podzemlja – pojavljivao se kao niotkud; bio je neverovatno arogantan, što nije bilo nimalo simpatično; ali više od svega, njegova motivacija da provodi beskrajne sate postujući poruke, vodeći često jalove rasprave i nervirajući sve ostale bila je potpuno nejasna.

Sve dok Mert Ortač nije otkrio da su dva najistaknutija korisnika turskog embrionskog interneta, BBS-a, nosila nadimke ChaO i Lord Cyric, niko nije ni počeo da slaže kockice.

Koristeći svoju osobenu mešavinu šarma i dvoličnosti, Mert se – postujući kao PilotM u kasno proleće 2007 – predstavio Lordu Cyricu kao neko sasvim treći, inače njihov zajednički poznanik. „Hej, matori!", poslao mu je poruku, „šta ćeš ti na ovakvom forumu?" Cyric je jedva dočekao da postavi isto pitanje čoveku koji se pretvarao da je njegov stari drug! Ubrzo su, međutim, zadovoljno ćaskali, pogotovo o pitanjima vezanim za enkripciju. Mert je primetio da je Lord Cyric izuzetno talentovan kompjuterista, što je potvrdilo Mertove sumnje o njegovom stvarnom identitetu. I posle nekoliko dana ili nedelja razmene ideja i informacija, Cyric je pristao da omogući virtualni susret između ChaO-a i Merta (koji se još pretvarao da je neko drugi). Koristeći enkriptovani ICQ mesidžing, Mert je počeo da ćaska sa ChaO-m (na turskom, razume se).

„Vidi", rekao je ChaO Mertu, „ne provodim mnogo vremena u Turskoj. Radije boravim u inostranstvu." Dodao je da ne voli baš mnogo svoje sunarodnike i da, kad god je moguće, izbegava da ima posla s njima. „Zovem se Šahin i govorim turski samo kad baš moram", rekao je. S Mertom je, međutim, hteo da razgovara na turskom, zato što su se upoznali preko Lorda Cyrica. „On i ja smo stari prijatelji", kazao je ChaO.

U aprilu 2007. ChaO je isterao Drona sa DarkMarketa, a s njim je otišlo i umeće izrade mikroprocesora za skiming uređaje.

Upitao je Merta bi li mogao da se prihvati toga i Mert je pristao. Sad se već sve ozbiljnije uključivao u ChaO-vu kriminalnu rabotu, što je značilo da dobija ono najdragocenije – poverenje.

Samo je Mert mogao da kaže da je bio blizak sa ChaO-m i Cyricom. Naravno, potonja dvojica nisu mogla sa sigurnošću da kažu jesu li razmenjivala poruke s Mertom, zato što se on predstavljao kao neko drugi. ChaO je izričito poricao da ga je ikad upoznao ili komunicirao s njim sve do onog sudbonosnog dana kad ga je oteo i preko *Habera 7* okačio njegovu fotografiju na internet.

Još je važnije to što niko u Turskoj ili igde drugde nikad nije potvrdio postojanje misterioznog Šahina. Osim Mertove tvrdnje, nema dokaza da Šahin postoji, uključujući i njihov susret na kraju. Međutim, Mert je bio u pravu što se tiče jedne bitne činjenice: prijateljstvo između Lorda Cyrica i ChaO-a datiralo je odavno.

Mladi Ortač je, dabome, još radio za Tursku obaveštajnu agenciju. Tako je većinu večeri, nakon što bi veći deo dana proveo u Foxu Turska pretvarajući se da radi, igrajući se na DarkMarketu ili izrađujući mikroprocesore za ChaO-vu ilegalnu industriju skimera, Mert izveštavao svoje instruktore o dnevnim otkrićima. Pričao im je o poljskom spameru zvanom Master Splyntr, o Grendelu, geniju za bezbednost, o Lordu Cyricu i ChaO-u, o pomoćnim serverima kojima administratori DarkMArketa upravljaju u raznim evropskim zemljama, i o aktivnostima DHKP/C.

Šta je još radio? Njegov šef u Foxu Turska polako je postajao sve podozriviji prema njemu. Palo mu je u oči da Mert zadatke koje dobija skoro nikad ne odradi do kraja, već da umesto toga naniže čitavu litaniju izgovora zašto ga nikad nema na radnom mestu. Tvrdio je da je ozbiljno bolestan, a u više navrata je pokušao i da pozajmi novac od kolega. Ako je već tako uspešan, pitao se njegov šef, otkud to da nikad nema para u džepu?

Jednog dana je saznao da je Mert zatražio od svih kolega da mu daju svoje lozinke. Navodno su mu trebale za veliko unapređenje sistema. Šef je, međutim, stopirao taj plan taman na vreme, posumnjavši da je Mert lozinke tražio iz nekih manje poštenih razloga.

Drugog dana, dok je ćutke motrio na Merta, video je na njegovom stolu gomilu kreditnih kartica. Kasnije je našao i dve lične karte s Mertovom slikom, a da se pri tom ni na jednoj nije nalazilo njegovo pravo ime, datum i mesto rođenja. Naposletku,

primetio je da Mert posećuje sajt sa detaljnim uputstvima kako se provaljuje u bankomat. Što se Mert duže zadržavao tu, to je njegova potreba za novcem bila veća – i to za velikim sumama.

Mert je upoznao Sanem – devojku iz snova koja ga je zanela. Sanem je jedina osoba na svetu koja može da potvrdi je li Mertova neverovatna priča tačna. A Sanem ćuti.

32.
Sladak život

Stadion Šukru Saradžolu u uzavreloj četvrti Kadikoj u azijskom delu Istanbula bio je popunjen do poslednjeg mesta za poslednju sezonsku utakmicu Fenerbahčea na domaćem terenu. Fenerbahče je već osvojio prvenstvo Turske, pa je ova utakmica te prelepe nedelje potraj maja bila bučna proslava za neke od najfanatičnijih fudbalskih navijača na svetu.

Prisustvovao joj je i Mert Ortač. Možda stvarno; možda samo u svojoj glavi.

Gore u VIP ložama vladala je iščekujuća i vesela atmosfera. Šahin i njegov poverljivi saradnik Čagataj Evjapan čekali su početak utakmice, predviđen za pet posle podne. Inače, fudbalski navijači u Istanbulu svrstavaju se među najfanatičnije u Evropi i podeljeni su u tri tabora. Dva, Galatasaraj i Bešiktaš, nalaze se na evropskoj strani grada, dok azurno-žuti dresovi Fenerbahčea leže preko moreuza, u Aziji. Šahin i Čagataj su bili odani navijači Fenerbahčea i posete prvog rodnom gradu obično su se podudarale s utakmicama – štaviše, imao je zakupljenu VIP ložu na stadionu.

Među prijateljima koje je pozvao na utakmicu bio je Mert; Šahin je rekao Čagataju da je on jedan od novih momaka angažovanih u njegovom poslu sa skimerima. Mert je njima pak predstavio svoju novu devojku, Sanem. Bio je opčinjen njome, dok je nju smesta opčinilo razmetljivo bogatstvo njegovih kompanjona.

Sanem je već znala profile nekih ljudi u VIP loži. Nije joj bilo teško da izvuče tajne iz Merta. Ne samo da je po prirodi bio brbljivac nego je i očajnički želeo da impresionira svoju mladu ljubavnicu, za koju je smatrao da je previše dobra za njega. To što je videla moćne ljude poput Šahina i njegovog dobro građenog pomoćnika Čagataja kako se šepure po VIP loži, sigurno je potvrdilo Sanem da mali Mert stvarno ima neke poštovanja dostojne kontakte. Ukoliko se, to jest, ta utakmica Fenerbahčea nije odigrala samo u njegovim snovima.

Život je za Merta bio dobar. On i Sadun počeli su da zarađuju ozbiljne pare iz prevare Akbanka. Kao aktivni doušnik Nacionalne obaveštajne službe, uživao je široki raspon zaštite, a ChaO, ključni igrač DarkMarketa, veoma ga je cenio. Međutim, važnije od svega bilo je to što je sve svoje dane i noći provodio s neverovatnom, prelepom devojkom koja je, činilo se, bila podjednako zaljubljena u njega.

Došlo je leto i Mert je odlučio da sreću što ga je tih meseci pratila kruniše odmorom u Antaliji, u vrlo popularnom hotelu *Adam i Eva*, čiji su dizajneri uspešno sparili veliki budžet s izrazitim neukusom. Predvorje u kom se smenjuju lajt-šou efekti oplakuju ogromni beskrajni bazeni, dok su sobe poznate po bezbrojnim ogledalima i pogodne za mnogo energičnog seksa. Ništa od svega toga nije jeftino. Smeštaj staje od 400 dolara za noć pa naviše, a gosti hotela su primetili da dodatne usluge mogu očas posla da „nakarikaju" ogroman račun. Međutim, za mlade, lepe i bogate u Turskoj, ovo je bila letnja destinacija snova.

Samo što su se prijavili na recepciji, Mert i Sanem su naleteli na Čagataja, koji je takođe provodio leto na jugu. Debeljušnom gospodinu s naočarima u čijem se društvu nalazio, Čagataj je objasnio da Mert pomaže ChaO-vom timu oko „administracije". Debeljušni gospodin se čkiljavo zagledao u Merta i potom uzviknuo: „Čekaj malo! Pa ja ovoga znam još otkako je bio klinac u kratkim pantalonama! Šta ti, kog đavola, tražiš u ovom poslu?" Mert je reagovao kao i uvek, kikotom i nestašnim osmehom.

Kad su se uputili prema svojoj sobi, Mert se prignuo i tiho rekao Sanem: „Znaš, onaj drugi lik? To je bio Lord Cyric." Sanem je htela da zna zašto je Cyric moćniji od ChaO-a. Mert ju je uveravao da nije tako, ali onda se setio da nju pre svega interesuje moć, pa tek onda novac.

Bio je zaljubljen i na sedmom nebu, imao je pune džepove para i poštovanje kriminalaca i obaveštajaca, a za spoljni svet imao je i impresivan posao rukovodioca IT odeljenja u Foxu Turska. I ne samo to, nego je leto provodio izležavajući se sa svojom seksi devojkom u hotelu *Adam i Eva*. Bolje od toga nije moglo da bude.

A nije ni bilo – osvrnemo li se unazad, avgust 2007. predstavljao je kratkotrajno zlatno doba u svetu snova Merta Ortača, kad su se projekcije njegove mašte konačno podudarile sa stvarnošću. Skoro odmah po povratku u Istanbul, situacija je počela da mu

izmiče iz ruku i, kad se leto pretvorilo u jesen, počele su da se šire mračne senke. Sanem i Mert su uobičajili da skoknu u skup šoping na mesta kao što je ostrvo Mikonos u susednoj Grčkoj. Umeli su da spiskaju hiljade evra dnevno, što je neminovno pravilo rupu čak i u Mertovom vrlo dubokom džepu. Njegova ozlojeđenost zbog onoga što je smatrao njenom raskalašnošću bila je ravna njenom sve većem ogorčenju zbog njegovih tajni i laži.

U tipično komplikovanoj epizodi, Mert je priveden zato što je navodno ukrao 5.000 evra od prijatelja Saneminog brata. Pritvor u kom je završio bio je za Fox Turska kap koja je prelila čašu, i dobio je otkaz. Nije slutilo na dobro ni to što je Nacionalna obaveštajna agencija najzad zaključila da je postao smetnja i da joj se više ne isplati da ga štiti. Odjednom se osećao vrlo ranjivo, a pri tom je i ostao bez dva važna izvora prihoda.

Kad su ga uz kauciju pustili da na slobodi čeka suđenje, on i Sadun su, zahvaljujući nerešenim slabim tačkama Akbankovog sistema, intenzivirali svoje karding aktivnosti. Očajanje je preraslo u nervozu, pojačanu jadom zbog saznanja da ga Sanem vara. Raskid koji je usledio bio je buran, praćen ogorčenim optužbama obeju strana. Mert je verovao da mu je ukrala velike sume novca. Ona pak mora da je mislila da je prosto poludeo.

Dok mu se svet naglo rušio, Mert je za Novu godinu otputovao na jug, kako bi razmislio o svom sledećem potezu. Usput je dobio još loših vesti – Sadun je bio uhapšen, a policija je već upala u Mertov stan i pretražila ga mašući nalogom za njegovo privođenje. Da je ostao u Istanbulu, već bi bio iza brave. Kao i obično kad bi se našao u gadnoj situaciji, Mert je odlučio da nastavi da kopa sve dok se ne zakopa u ilegalu.

Kad se pod lažnim imenom vratio u Istanbul, počeo je da smišlja strategiju za bekstvo. Upotrebivši jednu od svojih brojnih lažnih ličnih karata, izvadio je novi pasoš i obezbedio sebi francusku vizu tako što je podmitio službenika u konzulatu te zemlje. Zatim je zaobilaznim pravcem, preko Martinika u francuskim Karibima i Pariza, otputovao u Ales, uspavani gradić osamdesetak kilometara severno od mediteranske obale Francuske.

Mert je bio izolovan. Finansije su mu bile ograničene, jedva da je govorio koju reč francuskog i, što ga je još više uznemiravalo, nije imao stalni pristup internetu. Međutim, barem je mogao da se teši spoznajom da je bezbedan. I tako se Mert,

nemajući šta drugo da radi, predao dugotrajnom razdoblju odmora i opuštanja.

Nakon bekstva navrat-nanos od ruke turske pravde i teške svađe s bivšom devojkom, ubrzo je počeo da doživljava Ales kao dobrodošlo utočište. Prvi put posle više meseci, možda i godina, mogao je da raskrsti s poluistinama, prevarama, krađama i izvrdavanjima. Mogao je da prekine ekstremnu kompartmentalizaciju[45] koju su zahtevale njegove brojne onlajn i oflajn ličnosti i potraži svoju stvarnu suštinu – pod uslovom, naravno, da je još imao prepoznatljivu suštinu. Možda je kucnuo čas da predahne od ludila: čas da počne da živi pošteno, nađe pravi posao i smiri se pored neke dobre žene. Ako pametno odigra svoje karte, sve mu je to ležalo nadohvat ruke.

A onda se jednog jutra, negde oko osam sati, na njegovim vratima začulo kucanje.

Mert je ležao u krevetu i pijuckao kafu. Ovde u Alesu nikad nije imao posetioce i nije ih ni očekivao. Zagrnuvši se bademantilom odvukao se do vrata, otvorio ih i ugledao dvojicu muškaraca s rancima na leđima. „Zdravo, Merte! Kako si?", obratio mu se prvi na turskom. U znak odgovora, Mert je slabašnim glasom promrmljao: *„Je ne comprends pas..."*[46] „Daj, Merte", rekao je drugi na engleskom, „znamo ko si. U tvom je interesu da nas pozoveš da uđemo."

Dok su sedeli u kuhinji sa šoljama kafe u rukama, jedan od njih dvojice izvukao je fasciklu i spustio je na sto. Mert ga je dotle već procenio kao drugu generaciju turskih doseljenika u Ameriku, zato što je govorio kolokvijalni turski, ali s primetnim naglaskom i povremenim gramatičkim greškama. Onaj drugi, koji je uglavnom i pričao, bio je Amerikanac.

Izneli su mu alternative: „Ili ćeš nam pružiti bezuslovnu pomoć, ili će ova fascikla otići francuskoj policiji." Mert je prelistavao stranice sa spiskom francuskih kreditnih kartica koje su on i

45 (Psihol.) Unutrašnji sukob osobe nastao zbog postupaka suprotnih načelima do kojih ta osoba drži. Ako nije u stanju da ga reši, osoba teži da situaciju prevazide tako što sukobljene misli smešta u odvojene „odeljke" (eng.: *compartments*) i posmatra ih kao zasebne, nekonfliktne. Time miri nepomirljivo i omogućava sebi normalno funkcionisanje. (Dobar primer je preljuba, kad osoba ubedi sebe da je posredi „samo seks", bez ljubavi koja ostaje rezervisana za bračnog partnera – tako ne guši libido, a i dalje je verna bračnom partneru.) (Prim. prev.)

46 Fr.: Ne razumem. (Prim. prev.)

Sadun skimovali nakon što su se uvukli u kompjuterski sistem Akbanka. Dvojica muškaraca podsetila su ga da bi u Francuskoj, za prevaru sa samo jednom kreditnom karticom, mogao dobiti i do osam godina robije.

Bilo je uzmi ili ostavi, ali pre no što je pristao, Mert je zahtevao da čuje koga njih dvojica predstavljaju. „Američku kriminalističku službu", glasio je odgovor.

„I šta hoćete od mene?", nastavio je Mert.

„Hajde, Merte, pogodi!"

Iznerviran i osujećen, Mert je samo odmahnuo glavom.

„Ono što od tebe hoćemo jeste ChaO."

33.
Povratak u Had

Dok su razgovarali o ChaO-u i njegovom mogućem boravištu, Mertu je iz njihovih pitanja i komentara bilo jasno da ne znaju ChaO-v identitet, kao ni identitet Lorda Cyrica. Dvojica agenata rekla su mu da se mora vratiti u Tursku, ponovo uključiti u DarkMarket i isterati ChaO-a i njegove kolege na otvoreno. Još su ga više iznenadili kad su mu rekli da server DarkMarketa kontroliše njihov čovek, pa mu tako mogu bez teškoća pomoći da se vrati na forume.

Koliko je Mert uspevao da dokuči, FBI je sada hteo da krene na sve preostale glavne igrače na DarkMarketu: ChaO-a, Lorda Cyrica, Master Splyintra, Shtirlitza i Grendela. Nisu mu rekli kako to planiraju da izvedu, ali on je očigledno trebalo da doprinese svemu tome. Izgledi mu se baš i nisu milili, ali opet, nije ni robijanje u nekom od francuskih zatvora, za koje se pričalo da su među najsurovijima u Zapadnoj Evropi.

Američki agenti dali su Mertu neka maglovita obećanja i snabdeli ga telefonskim brojem i imejl adresom Lusi Huver, pomoćnice pravnog atašea u američkoj ambasadi u Istanbulu. Dobio je i imejl nalog, *sadinsider@gmail.com* (ime je odabrao Mert),[47] putem kojeg je mogao da joj šalje poruke.

Mertov boravak u Langedoku je druga epizoda iz njegovog sveta snova koju nije moguće proveriti i potvrditi. Tačno je, međutim, da je uspostavio kontakt sa Lusi Huver iz FBI-ja, koja se u to vreme nalazila u Turskoj.

U zemlju se vratio u martu 2008, posle dvomesečnog odsustvovanja. Morao je prvo da smisli plan akcije. Odlučio je da se obrati medijskoj kući *Haber 7* i ponudi joj intervju s obećanjem da će otkriti sve tajne sveta kardinga i DarkMarketa. Namerio je – mada možda ne baš mudro – da uplaši ChaO-a, da mu dâ do

47 *Sad insider* na engleskom znači „bedni (žalosni, jadni...) insajder". (Prim. prev.)

znanja da su informacije o njegovoj operaciji procurile i da se verovatno nalazi pod policijskom istragom.

Bezazlen kakav je bio – to je, uprkos svemu, još činilo sastavni deo njegovog karaktera – Mert je pretpostavljao da ChaO neće uspeti da utvrdi ko je tajanstveni haker koji novinarima nudi intervjue. Međutim, nije računao na to da će ga *Haber 7* kradom fotografisati u Mekdonaldsu u Kadikoju, gde su se sreli on i njihov reporter. Čim je ta fotografija objavljena, ChaO je znao ko je propevao. Glavni baja je imao Merta čvrsto na nišanu.

ChaO, Lord Cyric i ostali su izvesno znali da je Mert, s nalogom za hapšenje nad glavom i Sadunom iza rešetaka, podložan pritisku od strane policije. Intervju je samo podstakao te sumnje. Stoga je Mert, umesto da se direktno vrati na forum DarkMarketa, kontaktirao sa svojim drugom, mladim hakerom po imenu Mustafa, koga je ChaO takođe znao. Mustafa je pak, po svemu sudeći, jedva čekao da izbrusi svoje umeće u kulturi lake zarade, kardinga i sajber kriminala.

Njegova porodica je poticala iz Antalije, što je Mertu dalo izgovor da ode iz Istanbula, gde se nije osećao sigurno. Više od mesec dana ostao je na jugu, koji mu je i inače bio omiljeni deo zemlje.

Mustafa je na DarkMarketu radio pod nadimkom MYD i imao je dobar, funkcionalan odnos sa ChaO-m. Mert, međutim, nije znao da je Mustafa upozorio ChaO-a da ga ovaj, izgleda, progoni.

Mustafa se dogovorio sa ChaO-m da se sretnu u Istanbulu, i on i Mert uputili su se natrag na sever. Mert je redovno obaveštavao Lusi Huver o svom kretanju i javio joj je da se sprema za susret sa ChaO-m. Amerikancima je bilo potrebno da konačno vide kako ChaO izgleda i odrede mu koordinate i komunikacijsku infrastrukturu. Jednom je i Mert održao obećanje – vodio je Amerikance do njihovog plena. ChaO je bio naložio Mustafi da se s njegovim ljudima nađe ispred *Burger Kinga* nedaleko od železničke stanice Goztepe, koja se nalazi na azijskoj strani Istanbula, oko tri kilometra od stadiona Fenerbahčea.

Kad su stigli na Goztepe, zatekli su tamo Hakana Oztana, gromadu od čoveka koji je bio Čagatajev telohranitelj dok su zajedno robijali i sad je i Šahinu ponudio iste usluge. Telohranitelj ih je odveo u kuću zvanu Apartmani Sozdener, u četvrti Suadije, nastanjenoj bogatom srednjom klasom, oko tri kilometra daleko odatle. Sobe su bile oskudno nameštene i ne naročito udobne.

Hakan je naložio dvojici mladića da sede s mirom i sačekaju dok im se ne jave.

Kako više nije imao zaštitu koju mu je pružao otvoreni prostor, a još manje onu koju mu je ranije obezbeđivala Nacionalna obaveštajna služba, Mert se zabrinuo da Čagataj dolazi da ga kazni. Nije znao da mu je Mustafa, prema ChaO-vim uputstvima, ubacio u laptop trojanca koji je ChaO-u sada otkrivao sve njegove tajne, tu neprobojnu džunglu prevrtljivosti. ChaO nije bio samo vrhunski kriminalac; bio je i od onih što ne praštaju. Sad je imao čvrste dokaze da Mert radi za policiju. Mert je pretpostavljao (i iskreno se nadao) da je Lusi Huver nekako organizovala nadziranje stana, ali nije video nikakve znakove koji bi na to ukazivali. Prema tome, ako se pojave Čagataj, Šahin i Hakan, u bilo kojoj kombinaciji, bio je u ozbiljnom čabru.

U nedelju, 18. maja 2008, u deset sati pre podne, Mert je bio sam kad se oglasilo zvono na vratima Apartmana Sozdener. Otvorio je i na pragu ugledao Hakana. Njegov posetilac nije rekao ni reč već je žustrim koracima prošao pored njega i zatvorio vrata za sobom. Mert mu je vedro dobacio da ga je očekivao. Hakan ga je ljutito pogledao. „Samo minut", rekao je. Potom je otvorio vrata i u stan je ušao Čagataj. Mert je počeo da menja boje, da bi na kraju ubledeo.

Čagataj ga je gurnuo na stolicu i počeo polako da korača napred-nazad ispred njega, ritualno pevušeći: „Mert... Namert... Mert... Namert" – igra reči na turskom, u kojoj antonim reči *mert* (hrabar) glasi *namert* (kukavica).

Zatim se Mert našao na podu i počeli su da pljušte udarci nogama u njegov stomak, grudi i noge. Ušla su još dvojica rmpalija, bacila mu ćebe preko glave da ih ne prepozna i pridružili se batinanju. Mert je povremeno nazirao cev pištolja uperenu u njegovu glavu.

Onesvestio se. Kad je došao sebi, još je bio na podu, ali primetio je video-kameru koja je snimala sve što se događa. Preko trojanca ubačenog na Mertov laptop, ChaO je ne samo mogao da pristupi podacima o njegovoj povezanosti s Lusi Huver nego je saznao da je i Nacionalna obaveštajna služba koristila Mertove usluge (mada samo s delimičnim uspehom).

„Dobro, dakle", rekao je Čatagaj u stilu ceremonijal-majstora, pritisnuvši dugme za snimanje. „Sada ćeš lepo da nam ispričaš celu priču, od početka do kraja." I tako je Mert ispripovedao

svoju bajku *Iza ogledala*, završivši oko tri sata ujutru. Hteli su da znaju sve – o tajnim agentima, o kardingu sa Sadunom, o istraživanju DarkMarketa, devojci – ništa nisu izostavili.

Batinaši su konačno otišli na spavanje, s tim što je jedan uvek bio budan, kako bi se postarao da kišom udaraca i šutiranja probudi Merta ako ovaj slučajno zadrema.

U ponedeljak u podne telefonirao je Šahin i Čagataj je uključio spiker. Dotad je Mertova volja već bila slomljena. Pretpostavljao je da će ga ubiti. Nije se iznenadio kad mu je Šahin naložio da ponovi sve što je već rekao. Sve je bilo snimljeno. Na kraju je progovorio Šahin. „U redu, kucnuo je čas da budeš kažnjen", rekao je bez imalo ironije. „Hoću da uradiš sve što ti Čagataj kaže da uradiš, a ja ću proceniti ishod."

Čagataj je rekao Mertu da ustane i skine odeću. Bojeći se da su namerili da ga siluju, Mert je konačno pukao. „O, zaboga, prosto mi smesti metak u čelo", preklinjao je. „Šta mi ovo, kog đavola, radiš?"

„Umukni", odbrusio je Čagataj. „Nemaš razloga za brigu. Nismo mi nikakvi silovatelji. Zadrži te bokserice i prihvati kaznu koju smo ti odredili!" Dogovarajući se telefonom sa Šahinom, Čagataj je ispisao onaj čuveni papir na kom se Kier ili Mert Ortač žigoše kao izdajnik i taster. Tako je nastao mit o Kieru. Novinar iz *Habera 7* pronašao je na sajtu Mertovo ime zajedno s nadimkom Kier. U stvari, Mert nikad nije koristio to ime – njegov pravi nadimak glasio je SlayraCkEr. Međutim, nakon što je Čagataj snimio onu fotografiju, novinari, policajci i karderi širom sveta govorili su o Mertu Ortaču kao o Kieru, mada ga tako nikad niko nije zvao.

Posle foto sesije, Merta su ponovo srušili na pod i nabacili ćebe preko njega. „Ostani ovde još pola sata, a onda možeš da ideš", rekao mu je Čagataj. „Ostavljamo ti odeću, a novac ti nećemo dirati. Možeš da uzmeš i jednu ličnu kartu. Odsad pa nadalje – dok si živ – nemoj da bi ti na pamet palo da napišeš ime ChaO, jer ako to uradiš, nećeš stići ni da udahneš, a ja ću te već ščepati za gušu." Na kraju, Čagataj nije odoleo a da ne doda i ličnu notu: „Da je po mome, na licu mesta bih te ubio. Ali, njemu se dopadaš. Zato budi zahvalan i drži jezik za zubima." (Čagataju je, inače, bila smešna i sama pomisao da bi mogao poželeti da ubije nekoga kao što je Mert – koji je po njegovom mišljenju bio običan bedni dripac.)

Pola sata kasnije, prebijeni Mert Ortač je, sa svega pedeset dolara u džepu, izbauljao iz stana i uputio se na glavnu autobusku stanicu, odakle je uhvatio autobus za Izmir. Tamo će lizati rane i razmišljati šta sledeće da uradi. Bilo je očigledno: otići će u ilegalu. Tako je Mert nestao poslednji put – uhapšen je tek posle više meseci, u novembru 2008. pri pokušaju da pod lažnim imenom izvadi pasoš.

Još čudnih priča nastanjuje Mertov svet snova – ni stvarnost ni maštu – ali, za naše potrebe, ovde se završavaju.

34.
Pohvatani na legalu

Dok najzad nisu uhapsili Merta, inspektor Bilal Šen nije imao pojma je li haker u bekstvu, je li još u zatvoru ili je prosto mrtav. Znao je, međutim, da vreme nije na njegovoj strani. Jedino što je još ostalo ovom policajcu bilo je da efikasno i strpljivo nastavi da sužava krug oko ChaO-a. Konačno je imao fotografiju i broj čoveka koji je poslao skimer i bio je ubeđen da će ga to naposletku odvesti i do njegovog naredbodavca. Naime, ChaO-v potrčko koji je isporučio skimer upotrebljavao je jedan od telefonskih brojeva koje je prijavio u formularu transportne firme, pa je policija uspela da „trianguliše" osumnjičenog – drugim rečima, uspeli su da označe kojim je antenama za mobilnu telefoniju pristupao njegov uređaj. Ubrzo su stekli tačnu predstavu gde se čovek nalazi i kuda se kreće.

Nije prošlo dugo i viđen je ponovo, kad su uspeli da ga stave pod prismotru. Naravno, za samo nekoliko dana odveo ih je do vile u Tuzli, udaljenom predgrađu Istanbula, koje leži nekih dvadeset pet kilometara južnije niz azijsku obalu. Danas lokacija jedne od najvećih turskih pomorskih baza, ova oblast, nekada poznata po ribarstvu, bila je jedna od malo preostalih u gradu u kojoj nove građevine još nisu preuzele primat. Sa svojim prostranim kućama živopisne spoljašnjosti bio je to vrlo tražen kraj grada, nastanjen mahom bogatim porodicama.

Osumnjičeni ih je odveo do luksuzne vile s bazenom u dvorištu. Posle višednevnog nadzora, tim za prismotru je utvrdio da u vili živi više muškaraca. Međutim, Bilalu nije trebalo dugo da ustanovi ko je glavni među njima. Pretraživši evidenciju kriminalaca, ubrzo ga je identifikovao kao Čatagaja Evjapana.

Nekadašnji talentovani student elektrotehnike, Čatagaj je sad imao podebeli dosije. Prvi put je bio uhapšen 1998. pod optužbom za prevaru. Dve godine kasnije napravio je najveću pogrešnu procenu, kad su on i njegovi saradnici uhvaćeni kako koriste klonirane bele plastične kartice da izvuku novac iz bankomata u

luci Izmir. Pošto je odslužio pet od dosuđenih mu dvadeset sedam godina robije, izgledi za dug boravak u zatvoru bili su previše za njega. Tako je jednog majskog dana 2005. Čatagaj preskočio zatvorski zid i netragom nestao, postavši manje begunac a više duh.

Za svoje hapšenje 2000. krivio je ljude s kojima je tada radio – i bio je rešio da ne dozvoli da mu se to ikad više desi. Ako hoćeš da nešto bude urađeno kako valja, glasila je Čatagajeva filozofija, onda to uradi sam.

Naravno, shvatao je da je sajber svet, za onih pet godina koliko je on sedeo u zatvoru, pretrpeo značajne promene. Znao je sve o Murovom zakonu, koji predviđa da će broj tranzistora koji jeftinim procesom mogu da se smeste na integralno kolo, negde do 2015. nastaviti da se udvostručuje svake druge godine. Preveden u stvarni život, taj zakon znači da će gadžeti svake godine postajati sve pomodniji i ekscentričniji, kompjuterski programi složeniji, alatke hakera prepredenije, a plodovi njihovog truda tim sočniji. Stoga se potrudio da se prilagodi novim okolnostima.

Pre svega, trebao mu je novi sajber identitet. Čatagaj je nestao na gotovo četiri godine, njegovo ime na pasošu bilo je zamenjeno imenom jednog od njegovih podređenih, telohranitelja Hakana Oztana, a u etru je bio Cha-0 (izgovara se kao italijanski pozdrav). Prvi slog svog imena i nulu koristio je još od 1996, kad se prvi put pojavio na BBS-u. U to vreme, ChaO-v neverovatni bezbednosni sistem osiguravao je da ga niko ne može identifikovati. Na javnim forumima kao što su CrimeEnforcers i DarkMarket, ChaO je prodavao skimere. Privatno je prodavao neprobojne bezbednosne sisteme za korisnike kompjutera koji zaista nisu želeli da iko otkrije njihov identitet.

Ali sada je Bilal naleteo na njega. Međutim, uočiti ChaO-vu lokaciju bilo je jedno; prikupiti neophodne dokaze i izgraditi čvrst slučaj protiv njega bilo je već nešto sasvim drugo. Sudije i tužioci u Turskoj su s internetom upoznati još manje od svojih kolega u Zapadnoj Evropi ili Americi, a u gradu je već poslovao veći broj poznatih i skupih advokata, koji su brzo učili kako da to njihovo neznanje iskoriste za dobro svojih klijenata i svog bankovnog računa.

Čatagaj je uživao u letu – bio je društven tip koji je voleo da izlazi u provod s prijateljima. Često je bio pratilac lepim ženama, među kojima je, govorkalo se, bila i jedna smela članica saudijske

kraljevske porodice. Voleo je skupa pića, vrhunsku hranu i zabave na jahtama, i s godinama je nabacio nekoliko kilograma viška. Činilo se da ne žali da potroši na svoj mondenski način života.

Bilal je stavio pod prismotru mnoge ChaO-ve saradnike – gomilali su se dokazi da iza nadimka ChaO nije samo Čagataj Evjapan nego čitava kriminalna grupa koja je funkcionisala kao podmazana. To je bio organizovani kriminal, a ne neki *script kiddy* koji prvi put u životu hakuje servere,[48] i predstavljao je dokaz rastućeg trenda u svetu. Tradicionalni sindikati zločina su internet prevare dugo smatrali „lakim" kriminalom, koji skoro da nije ni zasluživao njihovu pažnju. Sada je to počelo da se menja. Pomolivši se iz svog originalnog inkubatora, u kom se nestašni gikovi kikoću i igraju, i izašavši u odrasliji svet stvarnih mafijaških struktura, sajber kriminal je postajao sistematičniji, efikasniji i svesniji potrebe za bezbednošću. Implicitno, Bilalova lovina je imala odgovarajuće veće resurse, pa je građenje slučaja zahtevalo da inspektor pažljivo vodi računa ako želi da izbegne da ga u sudnici zbune.

Policija je vredno prikupljala dokaze i, dabome, Kit Mularski i ChaO su još bili kolege administratori na DarkMarketu. Operacija je trajala punih pet meseci, a Bilal je za to vreme svakodnevno skladištio deliće dokaza. Utvrdio je da je Čatagajev poverljivi krug relativno mali, kao i da je njegovo obezbeđenje vojničko u svojoj preciznosti. Međutim, zajedno s tim delićima, koji su mogli povezivati Čatagaja s bilo kojim zločinom, Bilal je imao i nešto drugo na dnevnom redu: još je pokušavao da ustanovi da li Čatagaj ima nekog unutra – i istovremeno se molio da nema.

Krajem avgusta, Čagataj je nestao. Tim za prismotru se upaničio. Bez obzira na to, novinar *Habera 7* je nastavio da dobija poruke, ne od ChaO-a već od izvesnog Jarisa, koji je, izgledalo je, bio intimno upoznat s ChaO-vim aktivnostima. Srećom po Bilala, ChaO se pojavio u Istanbulu, isto onako neočekivano kao što je otišao. Ipak, bila je to opomena da je situacija više nego nesigurna i Bilal je odlučio da početkom septembra krene na njega.

Tim za prismotru vile u Tuzli utvrdio je da svakih nekoliko dana jedan od njenih stanara odlazi po provijant. Tako je bilo i

48 *Script kiddy, skiddie, skid, script bunny, script kitty* (pejor.) – najčešće adolescenti, ne poseduju potrebno tehničko znanje pa hakerske programe skidaju s interneta, uglavnom zato da bi se dokazali pred vršnjacima. (Prim. prev.)

osmog septembra. Bilal Šen se u međuvremenu vratio u Ankaru, gde je obuzet nervozom pratio dok su mu iz jedinice za specijalna dejstva, koja je opkoljavala kuću, telefonom iz minuta u minut prenosili tok operacije. Kad se čovek koji je izašao u kupovinu vratio, krenuli su u akciju – upali su u vilu i prikovali preostalu četvoricu na pod. Posvuda naokolo ležali su bezbrojni kompjuteri, desetine i desetine skimera, kalupa, PIN podmetača, uređaja za provlačenje kartica i hrpe gotovine. Prepad je bio više nego uspešan – niko nije povređen, a svi osumnjičeni su privedeni.

Čudno, ali nagoveštaj mogućnosti ChaO-vog hapšenja pojavio se nekoliko dana pre toga na forumu časopisa *Wired*, nakon što je jedan od novinara tog časopisa postavio na sajtu njihovog onlajn izdanja priču o DarkMarketu. Jedan od komentara ispod teksta poticao je od nekog ko je tvrdio da je Lord Cyric, administrator DM-a. Tvrdio je da je u direktnom kontaktu sa ChaO-m. I zagonetno je dodao da će neki od ChaO-vih podređenih možda i završiti iza brave, ali da ChaO nikad neće.

Zbogom, ChaO?

35.
Smrt DarkMarketa

Ko god da je ChaO zaista bio, neočekivano hapšenje Čagataja Evjapana je, čini se, posejalo paniku među njegovim kolegama administratorima na DarkMarketu. Šesnaestog septembra 2008, ni punu nedelju dana posle hapšenja u Istanbulu, Master Splyntr objavio je na sajtu DM-a da su uspesi policije istanjili živce njemu i ostalim administratorima, i da smatraju da nisu u stanju da nose taj teret:

> Očigledno je da ovaj forum... privlači previše pažnje mnogih svetskih službi (agenata FBI-ja, TS-a, Interpola). Pretpostavljam da je to bilo samo pitanje vremena. Žalosno je što smo se našli u ovoj situaciji, zato što smo... od DM-a napravili glavni forum za obavljanje posla na engleskom govornom području. Ali život je takav. Kad si na vrhu, ljudi pokušavaju da te povuku na dno.

Za samo nedelju dana, glavni kriminalni sajt engleskog govornog područja bio je mrtav. Njegove članove to je veoma uzrujalo. „DarkMarket je bio most preko koga smo poslovali, a ako je taj most srušen...", jadikovao je član po imenu Iceburg u postu na sajtu časopisa *Wired*. „Živeli keširanje i karding. Pocrkali dabogda svi TASTERI i FBI i glupave tajne službe koje ne samo da nam uništavaju život i porodice nego i sve što smo dosad postigli."

Izgledalo je da su sajber panduri pobedili. Međutim, kako govorimo o DarkMarketu, priča ipak nije baš tako jednostavna.

Deo IV

36.
Ni kriv ni dužan

Štutgart, septembar 2007.

Detektiv Ditmar Lingel bio je zadovoljan obavljenim poslom. Šef mu je pre nedelju dana dao logove dobijene od kanadskog veb-mejl provajdera *hushmaila*. Taj imejl sistem je navodno potpuno nepropustan – ako koristite *hushmail*, niko ne može da čita vašu prepisku. To je umnogome tačno, ali kompanija je 2007. popustila pod pritiskom kanadske policije i omogućila joj pristup svojim logovima. Oni su istražitelju otkrili koja se IP adresa logovala na određeni imejl nalog. A RCMP je logove za dva naloga, *auto432221@hushmail* i *auto496064@hushmail.com*, prosledila agentu Mularskom iz FBI-ja.

Pre toga, Matrix001 je u maju 2007. poslao Kitu Mularskom redigovanu verziju anonimnog imejla kojim ga je nepoznata osoba upozorila da ga nemačka policija drži pod prismotrom. Mularski je u prvi mah pretpostavio da su za curenje informacija krive kolege iz Tajne službe. U to vreme su, naime, federalci i Tajna služba uporedo vodili operacije usmerene protiv DarkMarketa, uvećavajući tako mogućnost da usled nesposobnosti ili zlonamernosti dođe do povrede obezbeđenja. Međutim, za Matrixa su znale i najmanje tri policije na drugoj obali okeana: Britanci, Francuzi i, naravno, Nemci.

Niko u policiji nije potcenjivao važnost tih imejlova. Pored mogućeg postojanja „krtice", bila je tu i uznemirujuća pomisao da je neko hakovao kompjutere jednog od istražiteljskih timova. Operacija DarkMarket se zahuktavala, ali hapšenja Matrixa i JiLsija bila su tek početak – plan je bio da je protegnu na nekoliko godina. Imejlovi su ugrozili čitavu strategiju sagrađenu tokom više od dve godine mukotrpnog rada. Curenje informacija je

moralo da prestane. Potreba da pronađu njegov izvor postala je prioritet ove međunarodne istrage.

Dolazak logova *hushmaila* na Lingelov radni sto značio je da može da počne detaljno proučavanje dokaza. Kao tehnički specijalista tima zaduženog za istragu Matrixa001, Lingel je imao zadatak da pokuša da pristupi tim nalozima otprilike u vreme kad ih je Matrix dobio.

Ustanovio je da je jedna IP adresa koja je pokušala da pristupi anonimnim *hushmail* nalozima poticala iz oblasti Štutgarta. Odmah ju je odbacio – bila je njegova. Nakon što je Kit Mularski upozorio Štutgart na postojanje tih imejlova, Lingel je pokušao da se uloguje na *hushmail* nalog koristeći neke standardne lozinke (kao što su *admin* ili *password*). Ostale su pak pripadale istaknutim DarkMarketarima koji su policiji bili već poznati. Drugi pokušaji logovanja poticali su s IP adresa u Berlinu i drugde u Nemačkoj. Dvanaestog septembra ujutru, u razgovoru sa šefom odseka Gertom Volfom, Lingel je objasnio da još nemaju osumnjičenog, ali da uspešno sužavaju potragu.

Posle ručka, Volf je provirio kroz Lingelova vrata i rekao mu da moraju da odu kod šefa uprave. Ušavši u kancelariju, Lingel je zatekao grupu starešina kako ga čeka, uključujući i šefa službe sa zlokobnim nazivom Dezernat 3.5, inače štutgarskog odseka za unutrašnje istrage.[49] Lingel je bio zbunjen i prilično nervozan. Šef pomenutog odseka je iznenada objavio: „Gospodine Lingel, od ovog časa ste pod istragom, zbog sumnje da ste obavestili osumnjičenog da se nalazi pod prismotrom."

Lingel je zanemeo. Potom je šok lagano počeo da ustupa mesto gnevu. „Eto ti sad", razmišljao je, „cele nedelje sam sa šefom radio na rešenju ove zbrke, a onda on posle ručka proviri u moju kancelariju i zabode mi nož pravo u leđa."

„Vidite, gospodine Lingel", nastavio je starešina, „možete da birate. Ili ćete sarađivati s nama u ovoj istrazi, ili ćete odmah biti smešteni u istražni zatvor."

Lingel je pristao da sarađuje. Njegov šef mu je objasnio da mora odmah iskoristiti sve preostale slobodne dane, posle čega će biti suspendovan do daljnjeg.

Sa svojih četrdeset i nešto, Lingel je imao prilično nekonvencionalnu prošlost. Rođen je u Vindhuku, glavnom gradu Namibije,

49 Nemačka reč *Dezernat* (izgovara se *decemat*) zapravo ima sasvim prozaično značenje – „nadleštvo". (Prim. prev.)

koja je kao deo Jugozapadne Afrike bila jedna od malobrojnih predstraža carske Nemačke u kolonijalnom razdoblju. Imao je pet godina kad se s roditeljima preselio u Kejptaun, tako da je odrastao tečno govoreći engleski jezik, kao i nemački. Na studije je otišao u domovinu svojih roditelja, a nakon što je diplomirao, počeo je da radi u policiji. Lepo je napredovao u hijerarhiji saobraćajne policije, mada nikad nije smatrao taj posao naročito izazovnim.

Kao gik amater, 2000. je oberučke prihvatio šansu da konkuriše za mesto u policiji Baden-Virtemberga. Štutgarskom štabu trebao je neko s iskustvom s open-source operativnim sistemom Linux, da vodi računa o bezbednosti mreže. Pet godina kasnije, dozvolili su mu da zajedno sa svojim kompjuterskim veštinama pređe u odsek za krivične istrage, gde mu je neposredni rukovodilac bio Frank Ajsman.

Matrix001 nije bio jedini Nemac koga je Kit Mularski identifikovao kao aktivnog člana DarkMarketa. Druga dvojica bila su Soulfly, pravo ime Mihael Artamonov, i Fake, pravo ime Bilge Ulusoy. Državni tužilac je u prvi mah pokušao da optuži Matrixa001 za kriminalnu zaveru, ali to je zahtevalo dokaze da je radio u dosluhu s ostalom dvojicom.

Iz nekog razloga, međutim, protiv Fakea i Soulflya nikad nije pokrenuta istraga i to je delimično razlog što je sudija u oktobru 2007. primorao državnog tužioca da odustane od optužbe za udruživanje u korist manje teške optužbe za prevaru s kreditnim karticama. Zašto nisu pokrenuli istragu protiv navodnih saučesnika u zaveri samo je prvo od više pitanja bez odgovora, koja su značajno narušila poverenje u Oblasnu i Federalnu policiju u Nemačkoj u pogledu istrage ovog slučaja.

A istraga badenvirtemberške policije u Štutgartu protiv Matrixa001 bila je opterećena mnogo čime. U međunarodnim slučajevima kao što je ovaj, obično se sva komunikacija filtrirala kroz Vizbaden, ali je glavni istražitelj Frank Ajsman ubedio pretpostavljene da bi trebalo da mu dozvole da komunicira direktno s Kitom Mularskim, ključnim čovekom iz FBI-ja.

Dakle, kad je Mularski čuo od Matrixa001 da je ovaj s anonimnog *hushmail* naloga dobio poruku s upozorenjem da mu predstoji hapšenje, usledilo je mnogo nervoze. A policije u Londonu, Pitsburgu i Štutgartu uglas su se molile da izvor, odakle god da potiče, nema nikakve veze s njima.

Posle Lingelovog hapšenja istražitelji su odahnuli – izgledalo je da je krivac uhvaćen. Ali, u decembru 2007. Dezernat 3.5 poslao je Lingelu dopis kojim su ga obaveštavali da nema nikakvih drugih dokaza koji ga povezuju sa slanjem spornog imejla i da od sledećeg meseca, u januaru 2008, može da se vrati na posao. Međutim, nije se vratio u Četvrti odsek, koji je vodio istragu protiv Matrixa001. Lingel je bio veoma ogorčen na svog neposrednog rukovodioca Franka Ajsmana koji je, činilo se, bez imalo oklevanja upro prstom u svog podređenog.

Dok se suđenje Matrixu, predviđeno za kraj proleća, polako približavalo, atmosfera u sedištu štutgartske policije bila je sumorna i vladao je razdor. Budući da protiv Matrixa nije moglo da podigne optužnicu za kriminalnu zaveru, tužilaštvo je bilo svesno da verovatno neće izdejstvovati zatvorsku kaznu. Štaviše, pokušaj da utvrde odakle su informacije procurile ponovo se našao na početku.

Premda je Lingel bio ozlojeđen zbog onoga što ga je snašlo, premeštaj u Prvi odsek ispostavio se kao savršeno prihvatljiv, a ponašanje novih kolega prema njemu bilo je uzorno. To je bilo olakšanje i dobrodošla promena posle meseci ispunjenih podozrivim pogledima.

A onda, u maju 2008, Lingel je ponovo uhapšen. Ovog puta, međutim, nisu ga optuživali za pisanje imejlova Matrixu. Lingel je bio optužen da je ugrozio tajni identitet koji je za potrebe istrage preuzeo agent FBI-ja Kit Dž. Mularski.

37.
Zoro bez maske

U junu 2008, baš dok je trajalo suđenje Matrixu, radijski reporter Kaj Laufen je prelistavao primerak Revije Masačusetskog instituta za tehnologiju i primetio članak o sajber kriminalu. Do tog trenutka, ovaj novinar istraživač iz Karlsruea u jugozapadnoj Nemačkoj nije imao predstavu da to postaje toliki problem. Zainteresovao se i odlučio da otkrije u kojoj meri sajber kriminal pogađa Nemačku.

Oprezan ali temeljit, Laufen je za početak proučio članove krivičnog zakona Nemačke koji se odnose na kompjuterski kriminal. Čim ih je pronašao, poslao je imejlove u pedesetak oblasnih i opštinskih sudova u zemlji, s pitanjem imaju li takvih slučajeva.

Dobio je samo nekoliko odgovora, a nekom zgodom se jedan od njih odnosio na slučaj prevare s kreditnim karticama pred lokalnim sudom u Gepingenu, varošici u Baden-Virtembergu, koja se nalazi nedaleko od mesta gde je živeo. Mladić po imenu Detlef Hartman čekao je presudu po osnovu trinaest optužbi za upotrebu kloniranih kreditnih kartica.

Priča nije zvučala naročito zanimljivo, ali Laufen je svejedno rešio da kontaktira sa oblasnom policijom u Štutgartu i uskoro mu je inspektor Frank Ajsman objasnio osnove sajber kriminala. Uzgred je rekao da je Četvrti odsek u istrazi protiv Hartmana imao pomoć FBI-ja.

Dan nakon što je Detlefu 2. jula dosuđena kazna od devetnaest meseci zatvora uslovno, Kaj ga je zamolio za intervju, u pismu koje je neuobičajeno poslao poštom umesto imejlom. Detlef i njegovi roditelji su se u prvi mah odupirali pokušajima novinara da razgovara s njim, ali posle tri meseca su popustili, pa se Kaj početkom oktobra našao s mladićem na kafi.

Kaj Laufen nije bio početnik. Rođen u severnoj Nemačkoj, deo detinjstva i mladosti proveo je u Brazilu, i tečno je govorio portugalski, španski i engleski. Radio je širom Južne Amerike i znao je ponešto o organizovanom kriminalu i gangsterima. Međutim,

jedva je verovao sopstvenim ušima dok ga je Detlef častio pričom o Matrixu001 i njegovim avanturama u virtualnom svetu, u kom se svi diče čudnim imenima i komuniciraju na hibridnom engleskom jeziku – delom gangsterskom, delom anarhističkom i delom tolkinovskim – dok kupuju i prodaju ukradene finansijske podatke.

Kaj je odmah shvatio implikacije ovog novog stila kršenja zakona. Uz pomoć interneta, počinioci su mogli da s udaljenosti od nekoliko hiljada kilometara zaskaču nepoznate žrtve koje mogu ili ne moraju otkriti da im je privatnost narušena a novac ili identitet ukradeni.

A opet, ako je to tako stoprocentno sigurno, pitao se Kaj, otkud to da je Detlef na kraju uhapšen? „Jednostavno", odvratio je ovaj. „Jedan od kolega administratora, s kojim sam mesecima sarađivao, bio je agent FBI-ja. Ušao mi je u trag i dojavio nemačkoj policiji." Novinar je pomislio kako mladić možda preuveličava sopstveni značaj, pa ga je upitao ima li kakvih dokumentarnih dokaza kojima bi to potkrepio. „Imam", rekao je Detlef. „Poslaću vam ih."

Nekoliko dana kasnije, Detlef je Laufenu poslao saopštenje tužilaštva o podizanju optužnice protiv njega, napisano jedinstvenim nemačkim pravničkim jezikom:

> Kao što je dokazano u istražnom postupku, ovaj administrator koji je u konačnoj analizi, najmanje od juna 2006. imao potpunu kontrolu nad svim transakcijama, bio je agent FBI-ja Kit Mularski, koji je u cilju prikupljanja preciznijih informacija o kupcima i prodavcima ponudio da hostuje server. Kao dokaz podnosim dokument br. 148, Fascikla I, u kojem gospodin Kit Mularski obaveštava istražnog službenika Regionalne policije Franka Ajsmana [*sic*], ovim rečima: *Ja sam Master Splyntr* [sic]. Da je korisnik Master Splyntr [*sic*] upravljao serverom, dokazuje dokument 190, imejl od Kita Mularskog datiran 09.03.2007: *On mi je platio za server.*

Kaj je bio prenerađen. Još jednom je pročitao rečenicu. *Ja sam Master Splyntr.* Ne samo da je Detlef Hartman bio u pravu što se ticalo toga da je FBI bio na njegovom sajber tragu, već je tužilaštvo navelo ime agenta *i* njegov alijas. Igri je bio kraj, a on, Kaj Laufen, otkrio je istinu o jednom od najistaknutijih svetskih

sajber policajaca. Do pre tri meseca gotovo nije ni čuo za sajber kriminal.

Kad je Kaj pozvao Nacionalnu alijansu za obuku sajber forenzičara u Pitsburgu, odmah su ga spojili s Kitom Mularskim, koji je, kao i uvek, bio veoma ljubazan. Međutim, kad je novinar pročitao rečenicu iz imejla - *Ja sam Master Splyntr* – na drugom kraju linije zavladala je grobna tišina. Kit je znao da je provaljen. Jedina svetla tačka bilo je to što ga je provalio radijski novinar iz jugozapadne Nemačke, pa su postojali neki mršavi izgledi da se vest, čak i u doba interneta, ne raširi mnogo dalje od granica Baden-Virtemberga. U duši je, međutim, znao da su ti izgledi zaista vrlo, vrlo mršavi.

Je li ovo procurilo s onog istog mesta?

Kaj Laufen nije znao da je komesar štutgartske policije po drugi put odobrio suspenziju Ditmara Lingela na neodređeno vreme. Ovom prilikom, međutim, sumnjali su da je detektiv namerno dostavio tužiocu ime i alijas Mularskog da ga ovaj uključi u svoje uvodno izlaganje. Lingelov cilj je, navodno, bilo da iznese u javnost identitet Mularskog i tako diskredituje FBI. Motiv, tvrdio je komesar, leži u Lingelovom nezadovoljstvu nekim policijskim metodama primenjenim u istrazi nad Hartmanom.

Optužbe protiv Lingela dobra su ilustracija za fundamentalne *različitosti u filozofiji kriminalističkih službi u Evropi i Sjedinjenim Državama*. Evropljani su skloni da izbegavaju operacije koje podrazumevaju infiltriranje agenata u kriminalne grupe kao riskantne, ali i kao moralno i zakonski pod znakom pitanja. Amerikanci ih, naprotiv, često koriste. U Americi traje usijana rasprava o *tome gde završava infiltriranje a počinje namamljivanje u klopku*. Neki policajci u Evropi smatrali su da se operacija DarkMarket graniči s namamljivanjem u klopku, naročito zato što se Tajna služba posebno trudila da podstakne članove da se za vreme njene istrage upuste u kriminalne radnje (u slučaju Drona).

FBI i Kit Mularski su *energično branili svoje postupke naglašavajući* kako je prisustvo Mularskog i njegovog tima na DarkMarketu omogućilo prikupljanje informacija – konkretno, o planiranom proširenju ChaO-ve operacije – što je, prema tvrdnjama Mularskog, sprečilo potencijalne gubitke od čak 70 miliona dolara.

Dok je dovršavao svoju radio-emisiju o ovoj neobičnoj ali važnoj priči, Kaja Laufena snašlo je iskliznuće diskusa. Gotovo potpuno nepokretan, novinar je bio primoran da provede dve

nedelje u krevetu. Došao je do zaključka da niko u Nemačkoj neće mariti za to što je FBI doprineo hapšenju nemačkog kardera i što je on, Kaj, otkrio identitet agenta. S druge strane, priča o DarkMarketu je u tek-medijima u SAD privukla veliku pažnju. U njima, a posebno u časopisu *Wired* iz San Franciska, mnogo se pisalo o tome, naročito posle dramatične otmice Merta Ortača u aprilu i kasnijeg hapšenja ChaO-a u septembru te godine.

Kaj je svim srcem verovao da bi trebalo da obelodani dokaz da je DarkMarket zapravo bio tajna operacija infiltriranih agenata FBI-ja. Međutim, baš kao što okean razdvaja kulturu čuvanja reda i zakona, tako razdvaja i etičke standarde nemačkih novinara i njihovih anglosaksonskih kolega. (Britanska policija je više evropska nego američka, ali su njihovi lovci na vesti još beskrupuloźniji od onih u Americi.)

U Nemačkoj se smatra da nije red objavljivati puno ime navodnih kriminalaca dok suđenje još traje, a nemački mediji se u mnogim slučajevima suzdržavaju od toga čak i nakon što su optuženici proglašeni krivima. Isto važi i za policijske agente na tajnim operacijama. Svima koji dobro poznaju angloameričke medije, ta pomisao je, dabome, potpuno strana.

Stoga, kad je Kaj Laufen početkom oktobra 2008. telefonom razgovarao s Kevinom Polsenom, urednikom zaduženim za bezbednost sajta časopisa *Wired*, rekao je da će mu dostaviti dokumentovane dokaze koji pokazuju da je kriminalistička služba provalila na DarkMarket. Priložiće i imejl u kom Kit Mularski priznaje svoju ulogu Master Splyntra, ali strogo pod uslovom da Polsen ne pomene ime Mularskog. U imejlu koji je potom poslao Polsenu, s priloženim skenovima dokumenata, Laufen je to još jednom ponovio, uz opomenu: „Spalite ovo posle čitanja!"

Polsen se drugačije seća toga: pristao je samo da izostavi Matrixovo pravo ime. On i njegov tim s vremenom su napravili impresivan posao ušavši u trag većini priča iz sveta sajber kriminala, uključujući i DarkMarket. Štaviše, uređivanju časopisa posvećivao se s istim nepopustljivim žarom kao svojoj nekadašnjoj profesiji hakera – karijeri koja se završila pred sudom. I tako Polsen nije spalio posle čitanja. Objavio je 13. oktobra, u ponedeljak. Master Splyntr je bio mrtav.

Kit Mularski je pak bio besan kao ris kad je *Wired* objavio njegovo ime – poverenje kardera koje je stekao bilo je smesta izgubljeno. Nekoliko nedelja pre toga zatvorio je forum DarkMarketa,

zato što je JiLsijeva registracija imena domena uskoro isticala. Da je Master Splyntr pokušao da je obnovi, neki radoznali haker mogao je iskoristiti mogućnost da dozna njegov identitet.

Operacija DarkMarket bila je uvodna faza dugoročnog plana da se kriminalistička služba infiltrira u svet sajber kriminala. Za petnaest meseci koliko je trajala pre objavljivanja imena Mularskog u časopisu *Wired*, FBI, SOCA i druge policijske službe koje su u njoj učestvovale vodile su računa da samo povremeno obavljaju hapšenja. Za razliku od taktike koju je Tajna služba 2004. primenila na Shadowcrew, namerno se nisu odlučili na masovnu čistku članova DarkMarketa. Master Splyntr je najozbiljnije nameravao da se vrati s još boljim ugledom, naoružan obimnom bazom podataka o karderima i njihovim aktivnostima. Taj plan je sad bio zatrt u korenu.

Ne samo da je sav trud Mularskog bio uzaludan – u izvanrednom primeru međudržavne saradnje između fundamentalno različitih policijskih snaga, uhvatili su jednu od najkrupnijih riba u svetu kardinga, ChaO-a, i pohapsili još desetine drugih, od kojih su neki već bili osuđeni, dok je većina još čekala suđenje.

Međutim, ni agent Mularski niti iko drugi nije bio u položaju da krivi Ditmara Lingela. Lingel, naime, nije dozvolio da identitet Master Splyntra slučajno dospe u sudska dokumenta vezana za Matrixov slučaj, kao što je tvrdio šef Dezernata 3.5.

Ta čast pripadala je detektivu Franku Ajsmanu, Lingelovom šefu, koji je kasnije priznao da je „napravio veliku grešku" time što je podneo taj dokument kao deo policijskog dokaznog materijala protiv Matrixa. Ajsmanova greška dovela je do toga da je Kaj Laufen identifikovao Mularskog i tako doveo do kolapsa dugoročne operacije protiv kardera.

Ditmar Lingel je, međutim, ostao suspendovan i od svojih poslodavaca nije čuo ni glasa sve dok ga Dezernat 3.5 nije u septembru 2010. obavestio da mu predstoji suđenje. Tužilaštvo je odbacilo neosnovanu tvrdnju da je Lingel namerno obelodanio ime Mularskog. Umesto toga, uskrsnula je prvobitna optužba da je dojavio osumnjičenom da se nalazi pod prismotrom.

Lingel se opredelio da ospori optužbe i kasnije tog meseca u Štutgartu je počelo najduže suđenje koje je igde održano u vezi sa DarkMarketom. Ironično je što se pred sudom nije našao niko od sajber kriminalaca (osim što su se Matrix001 i Fake pojavili kao svedoci), već je policija Baden-Virtemberga bila nahuškana

na jednog od svojih ljudi. Taj fascinantni događaj odigrao se pred šačicom ljudi u čistoj, maloj, anonimnoj sudnici u Bad Kanštatu, banji nedaleko od Štutgarta. Svedočenja desetak učesnika u drami bila su zaprepašćujuća, jer su otkrila mnoge greške i nedaće koje otežavaju policijski posao u Evropi, ali i u Sjedinjenim Državama.

38.
Ko si ti?

Istanbul, oktobar 2008.

Čagataj Evjapan je u zatvoru delovao opušteno. Tu i tamo bi pripadnik istanbulske policije šapatom rekao nešto o superpolicajcu koji avionom dolazi iz Ankare da ga sasluša. Najduže zadržavanje u pritvoru koje turski zakon predviđa za osobe osumnjičene za učešće u organizovanom kriminalu iznosi četiri dana. Zatvorenik je sa zanimanjem iščekivao hoće li se pojaviti taj glavonja iz glavnog grada.

Inspektor Šen je najzad stigao. Morao je da sazna samo jedno.

„Ko je ptičica? S kim iznutra pričaš? Samo to hoću da mi kažeš."

Zatvorenik je oklevao, a pogled mu je odavao očajničku rešenost.

„Ni sa kim."

39.
Putovanje u nepoznato

Posao inspektora Šena bio je završen. Posle hapšenja, slučaj je, kako nalaže turski zakon, predat tužilaštvu. Ali ako je Čagataj Evjapan ChaO, ko je onda Šahin, za koga je Mert Ortač uporno tvrdio je pravi ChaO? Je li Šahin bio samo plod Mertove mašte? Najzad, Mert je zaista bio poznat po sklonosti da kiti i domeće.

Međutim, koliko god da ju je u ovom slučaju nakitio izmišljotinama, fundamentalni aspekti Mertove priče bili su istiniti. Radio je za razne zvanične organizacije, uključujući i Obaveštajnu agenciju; bio je izuzetno talentovan programer, s posebnim umećem dekriptovanja smart kartica; zaradio je ogromne pare prodajući Digiturkove kartice, zbog čega je kasnije dospeo pod istragu; obasipao je novcem i provodima ljude koje je želeo da impresionira; krstario je forumima DarkMarketa koristeći Sadunove nadimke Cryptos i PilotM; letovao je sa devojkom u hotelu *Adam i Eva* u Antaliji; a Čagataj Evjapan ga je sasvim sigurno oteo i izvrgao poniženju.

Međutim, nije bio u stanju da ponudi baš nikakav dokaz za svoju glavnu tvrdnju, da je tajanstveni Šahin u stvari pravi ChaO-v identitet. Mert je pokazao tako detaljno poznavanje unutrašnjeg mehanizma DarkMarketa da ga je, ako je lagao, neka osoba ili organizacija morala snabdeti svim tim pojedinostima. Pitanje – koje uporno ostaje bez odgovora – glasi: zašto? I kome su pokušali da smeste ili da ga diskredituju time što su u čitavo zamešateljstvo ubacili i neverovatnog gospodina Ortača? Svakako ne Čagataj Evjapan, pošto ga Mertova priča predstavlja kao manje značajnog krimosa? Policija? Ili je to možda čovek za koga Mert tvrdi da je Lord Cyric, istaknuti pripadnik turske i globalne internet scene?

Čak i tako, Mertova istina je i dalje bila isto tako prihvatljiva i verovatna kao istina inspektora Šena. Ključ ne leži u identitetu Šahina ili Čagataja. On se krije u liku ChaO-a. Nema sumnje da je čovek koji je bio mozak fabrike skimera i administrator na

DarkMarketu bio Čagataj Evjapan. Pitanje je samo je li Evjapan kontrolisao celu operaciju ili je zastupao veći sindikat zločina.

Sve u svemu, turska policija je uhapsila nešto više od dvadeset ljudi koji su, kako nagoveštavaju dokazi, bili povezani sa ChaO-vom operacijom bilo kao deo najužeg kruga ili kao sateliti. Virtualni kriminalac je bio upravo to – ne stvarni lik, već amalgam pojedinaca s različitim znanjima koji su funkcionisali kao jedinica. Na isti način je ukrajinski osnivač CarderPlaneta, Script, shvatio da generički termin „karder" zapravo skriva mnoštvo različitih veština: neki su bili stvarni hakeri; neki su bili grafički dizajneri; neki su bili elektroničari koji su pravili skimere; neki su skimovali bankomate; neki su obavljali unovčavanje; neki su se starali o bezbednosti; neki su prikupljali informacije, ponekad za kriminalce, a ponekad za policiju.

Tako su obojica, i ChaO i Script, predvideli svet sajber kriminala posle DarkMarketa – udaljavanje od labavo povezane zajednice pojedinaca koji se iz čistog koristoljublja bave kriminalnim radnjama, a u pravcu mnogo sistematičnije kriminalne organizacije čiji članovi obavljaju specijalističke zadatke: spamovanje, pisanje virusa, pranje novca, baratanje botnetima i ostale suštinski kriminalne radnje u virtualnom svetu.

Stoga je možda „ChaO" bio samo operacija – svi skupa spojeni u jednog. ChaO je bilo kolektivno ime koje je u početku težilo da stekne makar delimični monopol u novoj industriji prevara s kreditnim karticama putem skimovanja. Plan je bio smeo i verovatno bi uspeo da nije bilo udruženih napora Kita Mularskog i Bilala Šena, kao i podrške koju su im pružile druge kriminalističke službe i određeni pojedinci.

Stepen u kom je ChaO, kao entitet, bio organizovan, snažno nagoveštava još nešto. Tradicionalna zločinačka bratstva donedavno su „bila sklona da posmatraju sajber kriminalce kao građane drugog reda", kako je to opisao jedan od vodećih sajber policajaca iz SOCA. Međutim, za vreme postojanja DarkMarketa, policijske snage širom sveta počele su da opažaju kako tradicionalne grupe za organizovani kriminal neočekivano iskrsavaju u istragama sajber kriminala.

Unutar samog DarkMarketa postojala su tri veoma dobro definisana kruga uključena u projekt. Prvi su sačinjavali administratori, moderatori i ostali koji su držali „birokratske" položaje na sajtu. To su najčešće bili ljudi koji su posedovali napredne hakerske

veštine i odlično su se razumeli u kompjutere. Pored toga, s izuzetkom ChaO-a, ili nisu zarađivali velike pare, ili su radili direktno kao policijski agenti ili tajni doušnici.

Drugi krug su uglavnom obrazovali vešti, iskusni kriminalci koji su mahom radili samostalno – kao Freddybb ili RedBrigade. Pokazivali su različit stepen poznavanja kompjutera i, ako sami nisu bili u stanju da reše tehnički problem, znali su kome da se obrate za pomoć. Ti ljudi su na forumima poput DarkMarketa bili manje upadljivi od administratora i njihove ekipe. Cilj im je bio da zarade što više mogu a da pri tom ne privuku pažnju na sebe, mada su se i oni povremeno uključivali u međusobno zadirkivanje i ćaskanje o karding zajednici uopšte.

Treći krug bio je stanište krajnje profesionalnih kriminalaca koji su bili takoreći nevidljivi – nepoznati sem preko mitova i reputacije među pripadnicima zakona i svojim kolegama karderima. Ti ljudi su čak bili iznad glavnih veletrgovaca kreditnim karticama i malverom – poput Ukrajinca Maksika, koga je sajber tim turske policije uhapsio 2007. u Antaliji. Najčuveniji (koji je, kako se veruje, najvećim delom snabdevao Maksika materijalom) jeste Rus poznat prosto kao Sim, za koga policija pretpostavlja da je zapravo još jedan vrlo efikasan sindikat. To su ljudi koji nikad ne izbijaju iz senke.

ChaO je bio fascinantan i važan zato što se banda nalik tradicionalnoj organizovanoj kriminalnoj grupi umešala u sajber kriminal velikih razmera i pokušala da utiče na funkcionisanje sajta kao što je DarkMarket. Bio je to prvi stvarni dokaz da sajber kriminal više nije domen samo građana drugog reda – počinjao je da privlači i neke krupnije ribe.

Organizovani kriminal tradicionalno igra veliku ulogu u Turskoj. Na primer, u kombinaciji s kurdskim i nekim balkanskim grupama, turske bande dominiraju veleprodajom heroina na području Zapadne Evrope.

Krajem 1996. u gradiću Susurluk desila se spektakularna saobraćajna nesreća. Među poginulima su bili načelnik Policijske akademije i lider desničarske terorističke grupe Sivi vukovi, koji se slučajno nalazio na Interpolovoj listi najtraženijih kriminalaca kao jedan od glavnih trgovaca drogom i poznati plaćeni ubica. Jedini koji je preživeo bio je poslanik tadašnje vladajuće partije.

Taj događaj omogućio je novinarima i opozicionim političarima da počnu da raspliću mrežu nasilja i prevara koja je povezivala

tursku Državu u državi s najuticajnijim pripadnicima grupa za organizovani kriminal. Godinama su uživali u uzajamnom prijateljstvu, gostoprimstvu i zaštiti. Priče o tome nisu zaprepastile samo običan svet u Turskoj već su dale i značajan podstrek snagama u usponu u turskoj politici – poput organizacije koja će naposletku prerasti u AKP i označiti borbu protiv kriminala i korupcije kao središnji deo svoje političke platforme.

Turska je otad ostvarila izvestan napredak. Međutim, kada koreni korupcije i organizovanog kriminala zadiru tako duboko kao što je to bio slučaj u Turskoj osamdesetih i devedesetih godina prošlog veka, potrebno je više decenija da se sasvim zatru u političkom životu države. To objašnjava strahove Bilala Šena kad je prvi put čuo da je ChaO možda pod zaštitom nekih moćnih figura establišmenta. Sasvim je moguće, kao što veruju neki od Bilalovih kolega iz kriminalističkih službi izvan Turske, da je ChaO koji je nastanjivao DarkMarket bio deo mnogo veće organizacije. Kriminalne grupe u Turskoj imaju prste u raznoraznim sektorima – pored trgovine drogom, Turska je glavni centar za trgovinu ljudima (takođe zbog blizine Evropske unije). Poslednje dve decenije, tamo se razvio i unosan zanat pranja novca.

Tako je Čagataj Evjapan, glasi njihova teorija, zapravo bio samo ađutant stvarnog glavnokomandujućeg u kriminalnoj organizaciji ChaO. Čagataj je bio potpredsednik zadužen za odeljenje sajber kriminala i pokorno je otišao u zatvor jer je, metaforički rečeno, „primao metak umesto gazde". Možda je glavnokomandujući te čete bio Šahin. Ako je tako, Mertov „Šahin" možda stvarno postoji, a inspektor Bilal Šen je i pored toga uhapsio pravog čoveka.

DarkMarket je u oktobru 2008. zatvoren, ali niko – ni pripadnici kriminalističkih službi niti iko iz redova kriminalaca – nema predstavu o njegovoj stvarnoj istoriji i značaju. Posle tri godine, samo je mali procenat od skoro stotinu uhapšenih širom sveta zaista izašao pred sud.

Pravni sistemi imaju velikih teškoća da prihvate krajnje tehničku prirodu dokaza za sajber kriminal i uhvate se ukoštac s njima, ali obrazac po kom se većina zločina počini u nekim sasvim drugim zemljama takođe predstavlja ogromnu barijeru za istragu i sudsko gonjenje prestupnika. Nejasnoća, sumnja, obmana i zabluda oduvek su igrali važnu ulogu u dokučivanju metoda organizovanog kriminala. A internet višestruko povećava njihovu moć.

40.
Podnevni ekspres

Zatvor Tekirdag, zapadna Turska, mart 2011.

Neodređeno zgodan muškarac u elegantnom crnom odelu i s kravatom pažljivo me je odmeravao dok je ulazio u omanju duguljastu prostoriju. Crne oči pod malčice dubljim zaliscima naglašavale su hipnotički pogled i jezik mi se načas prosto zavezao. Preda mnom je stajao čovek o kom sam skoro dve godine čitao, razgovarao i razmišljao. Sad kad sam ga konačno upoznao, najednom nisam uspevao da smislim ništa primereno što bih rekao.

Možda je protekle dve i po godine čamio u zatvoru, ali to nije uticalo na njegovo dostojanstveno držanje niti na to kako je brižljivo vladao sobom. Za tri i po sata koliko smo razgovarali, bio sam potpuno svestan da me intervjuiše baš kao i ja njega.

Moj prvi kratki boravak u Tekirdagu dogodio se 1976, neposredno pre objavljivanja knjige *Ponoćni ekspres*, koju je Alan Parker kasnije pretočio u vrlo uspešan film. Knjiga kazuje priču o Biliju Hejsu, mladom Amerikancu uhvaćenom u pokušaju da prokrijumčari drogu iz Turske. Stravične muke koje je pretrpeo u rukama sadistički nastrojenog zatvorskog čuvara šokirale su publiku u Evropi i Sjedinjenim Državama. Turska je u to vreme bila na glasu kao surova i nemilosrdna zemlja; štaviše, za vreme boravka tamo, dok sam spavao u svom šatoru, napala me je grupa siledžija, proprativši to zahtevima da stranci odu kući.

Trideset pet godina kasnije, približavao sam se zatvoru Tekirdag, kaznenoj ustanovi s maksimalnim obezbeđenjem, poput one u kojoj je robijao Hejs. Smeštena na blagoj uzbrdici, možda kilometar i po ispred mene, bila je okružena golim poljima što su se pružala dokle god je dopirao pogled. Iza debele zavese od gustog snega nazirao sam visoke blede zidine zatvora i stražarske kule

na kojima su se pomerale siluete ljudi naoružanih mitraljezima. Moj prvi utisak nagoveštavao je da se od vremena Parkerovog filma ništa nije promenilo.

Unutra, međutim, odahnuo sam shvativši da su se, barem u tom delu zemlje, zatvorski uslovi promenili do neprepoznatljivosti. Svi kažnjenici imali su u ćeliji televizor, tuš i tolaet. Hrana je bila malčice spartanska, ali nesumnjivo hranljiva i srazmerno ukusna, dok su se stražari ophodili učtivo, ne samo prema meni nego i prema kažnjenicima. Uslovi su u mnogome bili bolji od onih koje ćete zateći u većini britanskih zatvora.

U Tekirdagu je bilo nekih zloglasnih osuđenika, među kojima se nalazio i podstrekač ubistva Hranta Dinka, pisca jermenske nacionalnosti koga su ekstremisti ubili, pa, zato što je bio pisac jermenske nacionalnosti. Nije iznenađivalo ni što je zatvor udomljavao neke od najozloglašenijih turskih narko-bosova.

A među teroristima i mafijaškim donovima nalazio se i predstavnik najnovije vrste poslovanja s one strane zakona – sajber kriminala. Bilo mi je potrebno više od godinu dana da dobijem odobrenje za razgovor sa Čagatajem Evjapanom: morao sam da ubedim i turske vlasti i samog Evjapana. Mesecima je to izgledalo kao potpuno nemoguća misija. Kad sam jednog ponedeljka početkom marta 2011. iz Zatvorskog direktorata u Ankari dobio dopis kojim me obaveštavaju da će mi, pod uslovom da se Čagataj slaže, dozvoliti da se u sredu vidim s njim, mome zaprepašćenju nije bilo kraja. Posle toga, rečeno mi je, Čagataj će biti premešten i drugu priliku neću imati.

Turske vlasti nisu znale – a i da jesu ne bi marile – da je moj pasoš zakopan duboko u utrobi konzularnog odeljenja kineske ambasade u Londonu, u procesu odobravanja vize. Kineski činovnici su robotski odbijali svaki moj pokušaji da ga se domognem kako bih u utorak odleteo u Istanbul. Stoga sam kontaktirao sa zatvorom u Tekirdagu i preklinjao ih da mi dozvole da odložim intervju za dan kasnije. Obavestili su me da mi, doputovao ili ne doputovao, neće biti dozvoljeno da vidim ChaO-a ako naređenje da ga prebace dobiju pre četvrtka. Lov će biti završen.

Zbog toga sam bio izuzetno nervozan dok sam se u četvrtak pre podne, dan kasnije nego što je trebalo, probijao kroz mećavu što je besnela celim putem od Istanbula do Tekirdaga. Bilo je sasvim moguće da će mi po dolasku tamo saopštiti da sam propustio priliku da se susretnem sa ChaO-m. Posle podužeg čekanja,

sproveli su me kroz troja rotirajuća vrata od debelog čelika čiji je mehanizam imao biometrijski print mog dlana, i odveli kod direktora zatvora. Daleko od sirovine kakvu bi čovek možda očekivao, bio je šarmantan i prijazan. Rekao mi je da nisu dobili nikakvu direktivu iz Ankare i da ću s gospodinom Evjapanom moći da razgovaram u kantini, kad prođe ručak.

Naposletku su me sproveli do one omanje duguljaste prostorije. Čagataj Evjapan je obazriv ali samouveren. Baš kao što mi je i rekao Bilal Šen, njegovi instinkti će smesta znati da li pokušavam da se prepredenim pitanjima domognem nekih informacija. Podsetio me je na Džulijana Asanža, mozak koji stoji iza Wikileaksa – superpametan ali s nepokolebljivim ubeđenjem u sopstvenu intelektualnu superiornost, što katkada može da se shvati kao ekstremna narcisoidnost.

Kad sam izneo pretpostavku da je Lord Cyric Toni – debeljušni gospodin s naočarima kog je imenovao Mert Ortač – prasnuo je u smeh obojen dubokim prezirom. „Razgovarali ste s Turskom obaveštajnom službom, zar ne?", oštro je rekao. Na neki način, bio je u pravu: ako je Mert lagao (što je, budimo iskreni, vrlo moguće), tada mora biti da je Turska obaveštajna služba podmetnula čoveka s naočarima u njegovu priču.

Međutim, Čagataj je u razgovoru potvrdio neke vrlo bitne aspekte Mertove priče, uključujući i lokaciju apartmana u kom su posle otmice držali Merta, i razmenu poruka između Merta i službenice američke ambasade Lusi Huver. Takođe, spremno se složio s tim da je njegovo hapšenje još jednom bilo posledica greške u stvarnom svetu.

Pored sve svoje staložene inteligencije, ChaO je odavao da se nečega ipak boji – ironično, bila je to ista neizrečena briga što je mučila njegovog arhineprijatelja u turskoj policiji. Tvrdio je da mu je jedan od onih koji su ga saslušavali ponudio mogućnost prelaska u program za zaštitu svedoka. U zamenu za to, trebalo je da svedoči u istrazi Ergenekon. Tražili su da prizna kako je osnovao tajnu sajber mrežu za zaveru Država u državi u vojsci, obaveštajnim službama i medijima. Policija je glatko porekla da mu je ikad iznela takvu ponudu.

ChaO je odbio – poslednje što želi, baš kao inspektor Šen, jeste da se nađe u procepu između Države u državi i aktuelne vlasti. U sajberspejsu se to drugačije radi.

Čagataj je u razgovoru nagovestio da on i uski krug hakera razumeju ono što se dešava na mračnoj strani Mreže daleko bolje od ikog u vlasti. Stavio mi je do znanja da mu je cilj prosto bio da demonstrira beznadežnost pokušaja snaga reda i zakona da upravljaju internetom – tvrdio je da će uvek biti ljudi poput njega, koji su u prednosti u odnosu na ostale.

Neverovatno, ali izgledalo je da ga ne uznemirava boravak u zatvoru, kao ni činjenica da će možda morati da odsluži dvadeset dve godine preostale od ranije presude iz 2000. godine, da i ne pominjem sve dodatne optužbe koje će možda biti podignute protiv njega kao posledica njegove aktivnosti na DarkMarketu.

Kad smo načeli temu FBI-ja i Kita Mularskog, licem mu se polako raširilo prezrenje. „FBI nema ništa o meni. Ako ima, zašto Master Splyntr nije poslao informacije koje turska policija može da iskoristi da podigne optužnicu?", upitao je. „Umesto toga, sve što mogu jeste da pokušaju da iskoriste onog jadnika Ortača da me namame u klopku." Čagataj je potom ustvrdio kako je hakovao bazu podataka Mularskog i izvukao informacije koje je FBI prikupio o svim članovima DarkMarketa, uključujući i materijal o sebi.

Budući da se nalazi u zatvoru, Čagataj, razume se, nije mogao da dokumentuje svoje tvrdnje. Kazao je i kako je od početka znao da je Splyntr FBI (mada se DarkMarketu pridružio na JiLsijev poziv, u februaru 2006, kad je Master Splyntr već odavno bio na forumu) i kako se pridržava strategije da „prijatelje drži blizu, a neprijatelje još bliže" – otud njegova spremnost da sarađuje sa Splyntrom kao administrator.

Bila je to primerena tema za kraj razgovora. U suštini, priča o DarkMarketu je priča o dva čoveka – Čagataju Evjapanu i Kitu Mularskom, obojici s podrškom u vidu impresivnih timova i veza. ChaO nije bio tamo neki običan krimos. Iako je primarna svrha poduhvata bila zarada, Čagataj je, reklo bi se, smatrao da borba između njega i kriminalističkih službi ima dublji značaj, skoro kao da je težio da pokaže svoju superiornu sposobnost, a time i uzaludnost pokušaja tih službi da sprovode zakon u sajber spejsu. Upravo u tome leži snažan element prvobitnog anarhizma kulture gikova – bihevioralni obrasci i moralni kodovi menjaju se dok prelazimo iz stvarnog u virtualno. Pravila igre su drugačija i nova.

Agent FBI-ja izašao je kao pobednik, ali ta pobeda je bila za dlaku i ni slučajno bez ostatka. Tri godine posle zatvaranja Dark-Marketa, odjeci ovog neverovatnog kriminalnog poduhvata čuju se u zatvorima i sudnicama u nekoliko delova sveta. I, dabome, mnogi DarkMarketari još uvek krstare sajberspejsom.

Internet je transcendentalan izum koji se uvukao u mnoge delove našeg života i u sve prostorije našeg doma. Ali pripazite – negde, u nekoj virtualnoj ostavi, možda se krije Lord Cyric.

Epilog

Na prvi pogled, izgledalo je kao da je smrt DarkMarketa zadala gadan udarac internet kriminalu, ali nije. Tačno je, međutim, da je privremeno podmetnula klip u točkove nekih glavnih karding mreža, među kojima su ChaO-va operacija u Turskoj, Maksikova u Ukrajini i ona koju je Freddybb vodio u Engleskoj. Međutim, naravoučenije koje su ostali ozbiljni sajber kriminalci pre svega izvukli iz čitave rabote bilo je jednostavno: angažovanje na karding forumima kao što su Shadowcrew i DarkMarket, a naročito oni koji pripadaju engleskom govornom području i imaju ogromnu bazu članova, sada sa sobom nosi neprihvatljivi nivo rizika.

Već je bilo nekih dokaza da su članovi kojima je glavni cilj zarada, a ne povećanje ugleda, na DarkMarketu mnogo manje prisutni nego što su bili na Shadowcrewu. Broj postova koje ostavljaju ljudi kao što je Freddybb dramatično je opao od jednog do drugog sajta. Na sajtu Shadowcrew je postovao pedeset javnih poruka i dve stotine privatnih. Na DarkMarketu ih je ostavio petnaest odnosno dvanaest. Uspešno obaranje Shadowcrewa od strane Tajne službe SAD jasno pokazuje ranjivost ovakvih sajtova, a Freddybb je izvukao pouku: smanji svoju vidljivost.

Pored opasnosti da budu provaljeni, karding forumi su u svakom slučaju nadživeli svoju korisnost. Putem tih sajtova su kriminalci, tokom skoro desetogodišnje aktivnosti, uspostavili globalne mreže ljudi kojima mogu da veruju. Pronašli su sebi tržišta, bilo da su kupci ili prodavci nezakonito pribavljenih podataka i dokumenata.

Međutim, razotkrivanje Kita Mularskog kao Master Splyntra i otkriće da je DarkMarket jednim delom bio dobro postavljena policijska klopka, nesumnjivo su ubrzali smrt karding foruma. To je uništilo strategiju FBI-ja i njegovih partnerskih agencija u Zapadnoj Evropi. Plan je bio da Master Splyntr posle nekog vremena uskrsne kao pošteni karder koji je uspešno izvrdao svim pokušajima FBI-ja da ga uhvati, zbog čega zaslužuje još veći nivo poverenja među karding bratijom.

Umesto toga, reagujući na aferu DarkMarket, hakeri, krakeri i sajber kriminalci povukli su se još dublje u digitalnu ilegalu. Takođe, u biznisu je sve prisutnija specijalizacija . Hakeri i programeri malvera razvijaju dizajnerske programe koji ciljaju specifične sisteme ili traže određene informacije. Zatim ih prodaju grupi koja nadgleda upad u finansijsku instituciju ili račune njenih klijenata. Kad dobiju pristup novcu, javljaju se „mazgaru", pojedincu ili grupi koji angažuju „mazge" za prenos novca širom sveta. Na raznoraznim sajtovima nalaze se bezbrojni oglasi za posao koji ljudi mogu da obavljaju za svojim kućnim kompjuterom. Veliki broj tih oglasa daju mazgari. Mazgar od potencijalnih mazgi traži da mu stave na raspolaganje svoj bankovni račun, u zamenu za procenat od suma koje prolaze kroz njega.

Razlaganje kriminalne aktivnosti na ove zasebne delove otežava kriminalističkim službama da identifikuju šta se zapravo događa i ko s kime sarađuje. Mnoštvo najrazličitijih mobilnih uređaja i aplikacija takođe nudi silne mogućnosti sajber kriminalcima.

Još jedan veliki problem predstavlja i nagla ekspanzija korisnika interneta. Policija u Zapadnoj Evropi primetila je da veličina kineske kriminalne hakerske zajednice ubrzano raste. Sve donedavno, Prevara 419 ili Nigerijska šema (poznata i kao „advanced-fee fraud") bila je specijalitet zapadnoafričkih kriminalnih grupa, naročito Nigerijaca, ponosnih tvoraca onih bizarnih imejlova koji od primaoca traže da im podhitno pomogne da iznesu iz zemlje milione dolara koji su ostali iza upokojenog diktatora.

Prevara 419, nazvana po relevantnom paragrafu kaznenog zakona Nigerije, jeste prastari štos - koji čini srž priče u komediji *Alhemičar*, elizabetanskog dramskog pisca Bena Džonsona. U suštini, prevarant ubedi žrtvu da mu unapred plati manju sumu novca, na osnovu njegovog obećanja da će to žrtvi omogućiti da zaradi mnogo veću sumu. Potom pokuša da joj izmami još novca ili prosto nestane s prvom tranšom. Iako je ovo bilo moguće izvesti i u elizabetansko doba, tada je predstavljalo napornu rabotu. Internet ju je učinio krajnje unosnom, zato što kriminalac, uz upotrebu spam imejlova, može da priđe desetinama miliona ljudi. Šanse da pronađe naivčinu su neuporedivo veće.

Prevara 419 pojavljuje se u raznoraznim oblicima i veličinama. Ponekad stiže kao molba bogatim Zapadnjacima da priteknu u pomoć siromašnom afričkom detetu. Pisma, faksovi i imejlovi preklinju pogotovo Amerikance da doniraju sredstva za izgradnju

nove crkve ili pomoć pastvi – u tim slučajevima, motivacija žrtava je dobronamerna i podstaknuta milosrđem. Sledeći unosan plen za prevarante koji primenjuju Šemu 419 jesu osobe željne ljubavi, pogotovo sredovečne udovice i raspuštenice koje ulaze u virtualne veze sa mnogo mlađim zapadnoafričkim muškarcima, koji im polako iscede ušteđevinu kao avans za seksualnu vezu do koje nikad ne dolazi.

Prevare 419 šalju se danas i iz Kine, na kineskom i na engleskom jeziku. Nadopunjava ih drugi hakerski specijalitet Kineza, a to je krađa predmeta iz MMORPG-a, što je nespretni akronim za nespretno nazvane Massively Multiple Online Role-Playing Games,[50] kao što je *World od Warcraft*, ili „real life" igrice, kao što su *Second Life* ili *Habbo Hotel*. Sve te igrice imaju digitalne predmete koje se mogu zameniti za pravi novac, koji se ulaže u virtualnu robu i usluge, koje igrači mogu kupiti kako bi dodatno ulepšali doživljaj igranja. Mada nisu jedini, kineski hakeri su naučili da „kradu" ove digitalne stavke ili novac, koji posle mogu da pretvore u prave pare, koje vrede u stvarnom svetu. Kineski monumentalni informatički potencijal zasad je mahom neiskorišćen, a ipak, u većini sektora povezanih sa kompjuterskom bezbednošću u civilnom i vojnom životu, smatraju ga drugim po redu u globalnoj hijerarhiji svrstavajući ga odmah posle Sjedinjenih Država. Budući da Kina počinje da shvata taj potencijal, priroda interneta će se izvesno promeniti.

Kako bi se izborile s ovim rastućim pretnjama, vlade i industrija sada ulivaju stotine milijardi dolara u sajber bezbednost, bilo u oblasti očuvanja reda i zakona, zaštite intelektualnog vlasništva ili u vojnom domenu. Gotovo sav taj novac ulaže se u tehnologiju, a zamisao je da će to biti dovoljno da zaštiti internet od svih tzv. „kodnih smradova" (bad code ili code smell), malvera i virusa koji se šunjaju sajberspejsom vrebajući nezaštićene kompjuterske mreže kako bi ih napali.

Nasuprot tome, u pokušaje da se utvrdi ko i zašto hakuje ne ulaže se takoreći ništa. Niko ne pravi razliku između hakera s Wikileaksa, onih iz američke ili kineske vojske, onih iz sindikata zločina ili prosto običnih radoznalaca.

50 Masivna višekorisnička mrežna igra igranja uloga (izvor: http://sr.wikipedia.org/sr-el/MMORPG). Među gejmerima, našim i svetskim, popularnija je "skraćenica skraćenice", MMO. (Prim. prev.)

Međutim, hakeri su retka i vrlo posebna sorta. Njihov psihološki i društveni profil se generalno razlikuje od profila tradicionalnih kriminalaca, pre svega onih koji predstavljaju ključ za otvaranje nezakonitih poslovnih prilika na Mreži, ali nisu preterano zainteresovani za novac – drugim rečima, gikovi. Razumevanje njihovih sposobnosti i motiva za angažovanje na specifičnim aktivnostima, kriminalnim ili nekim drugim, bilo bi od ogromne koristi industriji bezbednosti, koja je prekomerno zavisna od tehničkih rešenja. U onim retkim prilikama kad kriminalistička služba ili privatni sektor uđe hakerima u trag, što dovede do njihovog krivičnog gonjenja i osude, malo se radi na tome da se ti prestupnici angažuju i usmere u dobrom pravcu. Umesto toga, krivično-pravni sistemi Evrope i Sjedinjenih Država teže da im nametnu duge zatvorske kazne i posle toga ograniče pristup kompjuterima.

To je velika greška, ako imamo u vidu njihov psiho-sociološki profil. Pre svega, trebalo bi uzeti u obzir njihove godine: većina hakera vrlo mlada počinje da se bavi aktivnostima za koje bi se u najbolju ruku moglo reći da nisu baš zakonski čiste. Poput Detlefa Hartmana, mogu biti namamljeni u nezakonite radnje na Mreži pre no što je njihov moralni kompas evoluirao do kraja i pre no što su u stanju da potpuno razumeju implikacije onoga što rade.

U stvarnom životu su često psihološki ranjivi, što znači da njihovo zatvaranje među stvarne kriminalce može da bude vrlo kontraproduktivno, kao što je bio slučaj sa Maksom Vižnom. Iako poseduje nepredvidljiv ego, svi stručnjaci se slažu da Vižn poseduje neverovatan mozak i dosad neviđeno razumevanje kompjuterske bezbednosti. U svetu u kom vlada oskudica specijalista za kompjutersku bezbednost i u kom se pretnje samo množe, smeštanje takve fenomenalne dragocenosti u zatvor ne deluje kao pametan potez. Ovim ne želim da kažem da bi hakeri koji su se upustili u nezakonite radnje trebalo da izbegnu kaznu, već da potreba za rehabilitacijom nije samo moralni imperativ za državu nego da potencijalno ima i znatnu praktičnu vrednost.

Nekadašnji haker Raul Kjeza vodi u Torinu mali istraživački centar pod nazivom Projekt profilisanja hakera (Hacker Profiling Project), koji finansiraju Ujedinjene nacije. Njegovo istraživanje temelji se na intimnom poznavanju hakerske zajednice i na odgovorima hakera na obimne upitnike koje im šalje. Prvi rezultati

njegovog rada daju neke važne putokaze u pogledu mentalnog sklopa hakera.

Najupečatljivija je rodna neravnoteža koja prožima ne samo protivzakonite sajber domene već i organizaciju i rad interneta kao celine. Ta tema je na stranicama ove knjige samo nagoveštena, ali svakako zaslužuje detaljnije proučavanje. Premda muškarci u celom svetu dominiraju u politici i ekonomiji, kada je reč o novoj tehnologiji, ta dominacija je ekstremna. Postoji, razume se, mnogo dinamičnih žena koje se bave novom tehnologijom i novim medijima, ali, statistički, one čine samo vrlo mali procenat: prema Kjezi, svega pet odsto. Hakeri su skoro uvek muškarci.

Drugi nalaz Kjezine studije glasi da je prosečni haker inteligentan ili veoma inteligentan. Zatim, uočio je da je incidenca hakera izrazito talentovanih za prirodne nauke – fiziku, matematiku i hemiju – veoma visoka i da iznosi blizu sto odsto. To obično ide zajedno s relativno lošim rezultatima u oblasti društvenih nauka.

Najzad, tu je i ključno pitanje međuljudskih odnosa hakera. U najvećem broju slučajeva – mada ne uvek – mnogo im je lakše da odnose stvaraju u bezličnom okruženju interneta, nego u stvarnom životu. Zanimljivo je zašto je tako.

Hakeri obično ulaze u taj svet kao adolescenti, baš u vreme kad velika većina ima teškoća u uspostavljanju odnosa, pogotovo sa suprotnim polom. Zato su, barem delimično, njihove teškoće u ovoj oblasti sasvim normalne. Međutim, Kjeza je ustanovio i da nenormalno veliki broj hakera opisuje probleme u komunikaciji sa porodicom, pre svega s roditeljima.

Nakon što sam pročitao Kjezinu studiju i proveo mnogo vremena intervjuišući različite tipove hakera, prisetio sam se rada Sajmona Baron-Koena, profesora razvojne psihopatologije na Univerzitetu u Kembridžu. Njegov pionirski rad na proučavanju autizma doveo je dubljeg razumevaja spektra muških/ženskih bihevioralnih obrazaca. U suštini, tipični muškarci ispoljavaju pojačanu sposobnost da „sistematizuju" spoljni svet, dok tipične žene ispoljavaju bolje umeće „uživljavanja". Ovim ne želim da kažem da sve žene loše čitaju mape i da su svi muškarci beznadežan slučaj kad nekog valja saslušati, već samo da oba pola imaju izrazitu tendenciju ka „sistematizovanju" (muškarci) ili „uživljavanju" (žene).

Baron-Koenovo dalje istraživanje dovelo je do otkrića veze između ekstremnog muškog uma, koji se u određenim okolnostima može opisati kao „autističan", i visokih nivoa testosterona kojima fetus može biti izložen u materici. Njegova hipoteza je kontroverzna, ali u mnogom pogledu ubedljiva i neosporno dragocena u proučavanju hakera i njihovih obrazaca ponašanja. Razume se, nisu svi hakeri autistični; štaviše, samo vrlo malo njih jeste (mada je nekim vrlo poznatima, kao što je Gari Makinon, koga u SAD traže zbog hakovanja u Pentagon, dijagnostikovan Aspergerov sindrom). Međutim, stvarno izgleda da odgovaraju mnogim kliničkim opažanjima koja je profesor Baron-Koen zabeležio kod ličnosti koje se nalaze daleko na „muškom" kraju spektra.

S napretkom istraživanja, ovo bi moglo značiti da će biti moguće identifikovati hakerski tip ličnosti među decom koja još idu u školu. Na taj način, vršnjaci i mentori mogli bi ih podsticati da razvijaju svoje veštine, dok im u isto vreme pružaju moralno vođstvo kako bi se njihove sposobnosti kanalisale u pozitivnim smerovima. Reč „haker" sklona je da ima pogrdan prizvuk. Međutim, sposobnost hakovanja je zapravo preimućstvo, lično i društveno. Kompjuteri i mreže nikad neće biti bezbedni ako ih ne štite vrhunski hakeri. Neki takvi pojedinci već rade na tome. Po mom iskustvu, devedeset odsto hakera umešanih u nezakonite radnje izrazilo je veliku želju da radi u okvirima zakonite industrije – a tu šansu im treba pružiti čak i ako su već osuđeni za krivično delo.

Adevale Taivo, poznat kao Freddybb

Prvog januara 2009. Kraljevski sud u Halu osudio je Adevala Taiva na četiri godine zatvora zbog udruživanja radi prevare u periodu od juna 2004. do februara 2008. Prethodnog novembra izjasnio se krivim po jednoj tački optužnice, nakon što je već priznao da je s bankovnih računa širom sveta na prevaru izvukao nešto manje od 600.000 funti. Sudija je preporučio da se Taivo, po odsluženju kazne, deportuje u Nigeriju.

Uz skraćenje kazne zbog dobrog vladanja, Taivo je mogao da izađe iz zatvora 29. avgusta 2010. Dve nedelje pre toga pojavio se pred sudom u Grimzbiju, gradu koji se u zalivu Hamber nalazi preko puta Hala. To saslušanje obavezno je u skladu s britanskim Zakonom o prihodu od zločina, koji predstavlja jedan od retkih

razumnih doprinosa Tonija Blera krivično-pravnom sistemu Britanije, jer državi omogućava da prestupnicima oduzme imovinu stečenu nezakonitim radnjama. Međutim, kraj jednog ozbiljnog slučaja pretvorio se u farsu. Tužilac je zaturio fasciklu s najvažnijim papirima, izazvavši neočekivanu reakciju bradatog sudije Grejema Robinsona, čije se prvobitno dobro raspoloženje sasvim pokvarilo. Izjavio je da nema nameru da zakazuje novi termin za saslušanje, zbog čega bi dve strane trebalo manje ili više odmah da se sporazumeju. To je Adevalu dalo odličnu monetu za potkusurivanje. Sudija je na kraju prihvatio cifru koja je jedva prelazila 53.000 funti, na koliko je spala početna procena od 353.067 funti. Taivo je izjavio da nema nameru da plati, što je značilo da će morati da odrobija još godinu dana. Sedmog aprila 2011. deportovan je u Nigeriju. Kao jedan od najinteligentnijih likova koji su se ikad udostojili da zađu na karderske forume, Taivo je zamalo uspeo da održi svoj dvostruki život nadarenog hemijskog inženjera i sajber kriminalca.

Detektiv Kris Doson

Detektiv Kris Doson je veoma vredno radio na slučaju Freddybba, posvetivši i mnogo svog slobodnog vremena tome da osigura da haotična gomila cifara, datuma i tehnoloških detalja bude razumljiva svakom laiku kad konačno dospe pred sud. U pauzi zbog konsultacija za vreme saslušanja Taiva na osnovu Zakona o prihodima od zločina, Dosonu se učinilo da je čuo ovoga kako kaže: „Zajebi, nema šanse da platim." Kad je sudija napustio sudnicu, inspektor je otišao, obuzet gnevom izazvanim nesposobnošću engleskog sudskog sistema.

Kris Doson i dalje radi kao inspektor u odeljenju za ubistva u Halu.

Dimitrij Golubov

Posle hapšenja u Odesi, haker Dimitri Golubov proveo je u zatvoru pet i po meseci. Za to vreme su ga saslušavali pripadnici američkih kriminalističkih službi, među kojima je bio i Greg Krab iz Poštanskog inspektorata SAD. Međutim, posle intervencije dvojice

poslanika ukrajinskog parlamenta, pušten je iz zatvora, a sud u Kijevu ga je 2009. oslobodio svake krivice.

Visok skoro 190 centimetara, sa harizmatičnim pogledom plavih očiju, Golubov negira svaku povezanost sa Scriptom, iako je njegova verzija događaja puna nedoslednosti, a digitalni dokazi koje poseduju američki agenti kazuju sasvim drugačiju priču (među njima su i podaci pronađeni na kompjuteru Romana Vege, prema kojima su Script i Golubov jedna te ista osoba).

Script se izgubio ubrzo posle njegovog puštanja na slobodu, ali se Golubov vratio s obnovljenom posvećenošću društvenim promenama i preduzetno osnovao Internet stranku Ukrajine. Još uvek nastanjen u Odesi, sastavio je politički program koji za cilj ima borbu protiv korupcije, pornografije i trgovine drogom na internetu. Siguran je da će najduže za deset godina biti izabran za premijera ili predsednika Ukrajine i, mada šanse za to ovog časa izgledaju vrlo mršave, njegovu preduzimljivost i ambicioznost bi svakako trebalo shvatiti ozbiljno. Internet partija je imala desetine kandidata na lokalnim opštinskim izborima u Odesi i mada je zasad osvojila samo jedno odborničko mesto, neosporno je da se pokret širi po celoj zemlji.

Čudno je, međutim, da je Golubov, uprkos čvrstim moralnim stavovima svoje organizacije u vezi s nekim kriminalnim aktivnostima, kao što je dečja pornografija, pokrenuo kampanju za oslobađanje zloglasnog kardera Maksika, koji je u Turskoj osuđen na trideset godina zatvora.

Roman Vega

Roman Vega nalazi se u zatvoru od 2003. kad je uhapšen na Kipru. U junu 2004. je na zahtev SAD prebačen u Kaliforniju, i otad se nalazi u pritvoru a da mu nikad nije suđeno. U vreme pisanja ove knjige, on je pitomac Gradskog kaznenog zavoda u Bruklinu, sumorne ustanove nedaleko od zaliva Govanus. Za sve ovo vreme Vega nije imao drugih posetilaca sem svojih advokata.

U avgustu 2007. bilo je zakazano saslušanje pred sudijom Čarlsom R. Brejerom u Severnom distriktu Kalifornije. Tužilaštvo i odbrana bili su spremni da potpišu nagodbu, posle koje je Vega imao da bude pušten, budući da je već odslužio četrdeset šest meseci zatvora na koliko je pogodba glasila. Dan pre njegovog

puštanja, pred sam kraj radnog vremena, tužilac iz Istočnog distrikta Njujorka podigao je novu optužnicu s nizom tačaka, zahtevajući prebacivanje Vege u Bruklin. Te optužbe su u suštini bile identične onima u Kaliforniji. Njujorško tužilaštvo je, međutim, optužnicu podiglo pozivajući se na drugi zakon, kako bi izbeglo poništenje zbog nemogućnosti da se istoj osobi dvaput sudi za isti prestup (tzv. „double jeopardy").

Iz zapisnika sa saslušanja jasno je da je sudija Brejer, brat člana Vrhovnog suda Stivena Brejera, bio ljut i postiđen zbog taktike njujorškog Istočnog distrikta. Nova optužba temeljila se na informacijama dobijenim od agenata Tajne službe SAD.

Po Veginom dolasku u Bruklin, Tajna služba mu je ponudila nagodbu: pristane li da svedoči protiv Dimitrija Golubova i ostalih članova ukrajinskog establišmenta (ne hakera, dakle, nego istaknutih političkih ličnosti), povući će optužbe protiv njega. Međutim, ako odbije, objediniće ih s ostalim optužbama protiv njega podignutim u neki drugim državama SAD. Nastaviće tako sve dok ne bude pristao na saradnju.

Bez obzira na to šta je Vega uradio ili nije uradio, već je proveo u zatvoru tri puta više vremena nego oni iz Shadowcrewa koji su osuđeni za ista dela; pri tom mu dva nerešena slučaja još više nad glavom, a posredno mu preti još nekoliko. Vega pati od uznapredovalog propadanja zuba, trpi konstantne bolove i često nije u stanju ni da jede. Zatvorske vlasti i Maršalska služba SAD odbile su njegovu molbu da mu se ukaže medicinska pomoć.

Nema izgleda da će Vega u dogledno vreme biti pušten na slobodu.

Maksim Kovalčuk, poznat kao Blade

Kovalčuk je maja 2003. uhapšen na Tajlandu i isporučen Sjedinjenim Državama, gde je odslužio kaznu od četiri godine zatvora. FBI je pristao na postignutu pogodbu i on je potkraj 2007. pušten na slobodu, posle čega se vratio anonimnom životu u Ukrajini. Odluka FBI-ja da ga oslobodi u izrazitoj je suprotnosti s taktikom zadržavanja koju Tajna služba primenjuje u slučaju Romana Vege.

Renukant Subramanijam, poznat kao JiLsi

Dvadeset šestog februara 2010. Subramanijam se izjasnio krivim po jednoj tački optužnice za prevaru s kreditnim karticama i po četiri tačke optužnice za prevaru sa hipotekarnim kreditom, za šta ga je sudija u Kraljevskom sudu u Blekfrajarsu osudio na četiri godine zatvora. U vreme pisanja ove knjige, on je kažnjenik u zatvoru Vormvud Skrabs u Zapadnom Londonu, u kom su svojevremeno robijali kompozitor ser Majkl Tipet i gitarista Rolingstonsa Kit Ričards.

Uz smanjenje kazne zbog dobrog vladanja, očekuje se da će Subramanijam biti pušten potkraj jula 2012. Glavni deo njegovog slučaja nije povezan sa DarkMarketom već s prevarom sa hipotekarnim kreditom. Tužilaštvo je uključilo pet takvih pokušaja ostvarivanja finansijske koristi (mada su finansijske ustanove odbile tri od tih pet molbi za dobijanje kredita). Premda su te prevare prestup same po sebi, tužilaštvo je iznelo pretpostavku o povezanosti Subramanijamove zarade od DarkMarketa i njegove sposobnosti da otplaćuje rate kredita. Subramanijam pak tvrdi da nije odgovoran za otplatu kredita, jer je konkurisao u ime prijatelja koji to nisu mogli da urade. Pored toga, Subramanijam čeka i ishod saslušanja pred većem za prihode od zločina, da vidi da li će se od njega tražiti da još nešto plati. Prema uslovima njegovog Naloga o prevenciji zločina, pet godina posle puštanja iz zatvora neće smeti da koristi kompjuter bez nadzora.

Detlef Hartman, poznat kao Matrix001

Devetog oktobra 2007. Regionalni sud u Štutgartu doneo je odluku da bi Hartmanu trebalo suditi po trinaest tačaka optužnice za prevaru s kreditnim karticama. Međutim, isti sud odbacio je optužbu o učešću u kriminalnoj zaveri. Kako je ta ozbiljnija optužba odbačena, Hartmana su pustili iz zatvora Štamhajm, u kome je proveo prethodna četiri meseca. Ključna odluka, koja je sprečila njegovo krivično gonjenje na osnovu optužbe za zaveru, ležala je u načinu na koji je sud protumačio odredbu nemačkog Ustava prema kojoj se učesnik u zaveri mora osećati kao deo „ujedinjene grupe", u kojoj se pretpostavlja postojanje „podređe-

nosti pojedinca volji kolektiva". Sudija je obrazložio da fluidna priroda interneta i članske strukture DarkMarketa ne ispunjavaju te kriterijume – presuda koja, dabome, ima važne posledice za razvoj nemačkih zakona koji se odnose na internet kriminal.

U julu 2008. Hartman je osuđen na kaznu od dvadeset jednog meseca zatvora uslovno, po optužbi za prevaru. Posle toga je nastavio svoje studije grafičkog dizajna i potpuno prekinuo sve veze sa podzemljem.

RedBrigade

Vratio se poštenom životu i trenutno živi u Evropi.

Maks Vižn, poznat kao Iceman

Dvanaestog februara 2010. sud u Pitsburgu osudio je Maksa Vižna na trinaest godina iza rešetaka, što je najduža zatvorska kazna za hakovanje koju je ikad izrekao neki američki sud. Tužilaštvo je izračunalo da je njegovo hakovanje rezultovalo gubicima na kreditnim karticama u iznosu od preko 85 miliona dolara. Vižn se nalazi na izdržavanju kazne u Federalnoj kaznenoj ustanovi Lompok u južnoj Kaliforniji, zatvoru s minimalnim obezbeđenjem, gde mu nije dozvoljen pristup nijednoj vrsti kompjutera.

Vižnovo hakersko znanje nema premca – on je neosporno jedan od najinteligentnijih ljudi koji trenutno robijaju u Sjedinjenim Državama. U jesen 2010, na zatvorenoj konferenciji raspravljao sam o njegovom slučaju s jednim od najviših zvaničnika Ministarstva za unutrašnju bezbednost koji se bave sajber pretnjama. Složio se sa mnom da je to što kompjuterski stručnjak Vižnovih sposobnosti čami u zatvoru verovatno prava zloupotreba ljudskih resursa SAD, ali je naglasio da je Vižnov ego – koji je veliki gotovo koliko i njegov intelekt – takođe odigrao veliku ulogu u celoj stvari.

Nikolas Jele, poznat kao Dron

Jele je pušten iz zatvora nakon što je odslužio kaznu za prevaru s kreditnim karticama i ilegalnu proizvodnju skiming uređaja.

Hakim B, poznat kao Lord Kaisersose

Lord Kaisersose je u Marseju, gde još čeka suđenje, ali je pušten uz kauciju. Francuska je još jedna zemlja u kojoj bi točkovima pravde dobro došlo malo podmazivanja.

ChaO

ChaO upravlja sopstvenim biznisom u Sloveniji ili je u zatvoru, što zavisi od toga ko je pravi ChaO – Šahin ili Čagataj Evjapan. Potonji je u pritvoru u jednom od najobezbeđenijih turskih zatvora, onom u Tekirdagu. Njegovo suđenje predviđeno je za ovu godinu, ali je tužilaštvo odbacio one ozbiljnije optužbe koje se odnose na organizovani kriminal.

Mert Ortač, poznat kao SlayraCkEr

Mert se nalazio u pritvoru u Istanbulu i čekao je suđenje za slučaj Akbank, kad je u martu 2010. pušten zbog tehničkog propusta. U novembru 2010. ponovo je uhapšen i, u vreme nastanka ove knjige, još je u pritvoru. Mada ćudljiv i nepredvidljiv, Mert je jedan od najtalentovanijih likova umešanih u DarkMarket.

Kit Mularski i Bilal Šen

Obojica ponovo patroliraju opasnim ulicama sajbera.

Lord Cyric

Ko je on? Lov se nastavlja...

Napomena o izvorima

Glavnina informacija u ovoj knjizi potiče iz nekih dve stotine sati intervjua koje sam obavio od 2009. do 2011. Leonida Krušelnicki je takođe posvetila više sati vođenju intervjua.

Pored toga, oslanjao sam se na dva glavna dokumentarna izvora. Prvi su zapisnici s više suđenja povezanih sa slučajevima sajtova CarderPlanet, Shadowcrew i DarkMarket. Drugi su arhive pomenutih sajtova, pogotovo prva dva, koji su dostupni na internetu. Arhiv DarkMarketa, nažalost, nije u toj meri dostupan. Znam samo za jedan, a taj se nalazi u posedu FBI-ja koji, iz operativnih razloga, nije u mogućnosti da ga obelodani.

O temi sajber kriminala, sajber industrijske špijunaže i sajber ratovanja postoji obimna literatura, čiji se veći deo može naći na internetu. Moram istaći rad Kevina Polsena i njegovog tima, čiji je blog *Threat Level* (*Nivo pretnje*) dobro napisan i temeljito istražen. Želim da preporučim dve knjige koje se bave baš sajber kriminalom, Polsenov *Kingpin* i *Fatal System Error* Džozefa Mena. Za širi uvod u neke izazove koji se javljaju kao posledica internet tehnologije, obavezno bi trebalo prvo pročitati *The Future of Internet: And How to Stop It*, autora Džonatana Zitrena.

Među istinski dragocenim blogovima su i *Krebsonsecurity*, Brajana Krebsa; *Cryptogram*, bilten Brusa Šnajera; blog finske kompanije za kompjutersku bezbednost F-Secure; i blog Danča Dančeva i Rajana Narejna na Znetu, *Zero Day*.

Reči priznanja

U pisanju ove knjige suočio sam se s mnogim izazovima, kojima nikad ne bih dorastao da nije bilo velikodušne pomoći koju su mi pružali brojni prijatelji i kolege iz celog sveta.

U Britaniji je ključnu ulogu odigralo dvoje ljudi. Leonida Krušelnicki se ispostavila kao neumorni istraživač, često otkrivajući vitalno važni materijal dugo nakon što sam ja već odustao od svake nade da ću ga pronaći. Da nije bilo njenog truda, ova knjiga bi bila znatno siromašnija. Vesna Vučenović se postarala da se upravljanje ovim projektom odvija što je moguće bezbolnije.

Na svojim putovanjima imao sam sreću da upoznam dvoje novinara čije su strpljenje i vedrina ravni njihovom profesionalizmu i umeću, koji su zaista najvišeg reda. Kaj Laufen mi je pomogao da shvatim složenosti nemačke pravde. Međutim, njegov doprinos je i veći od toga, zbog kontakata koje mi je pomogao da stvorim i ponuđenog gostoprimstva. Isto tako, potpuno bih se izgubio u Istanbulu i Turskoj da nije bilo Šebnem Arsu, uporne, uvek učtive i sposobne da pronađe rešenje i onda kad izgleda da je sve izgubljeno. Njen sam veliki dužnik.

Od brojnih kriminalističkih službi s kojima sam razgovarao o DarkMarketu, moram izdvojiti agenta Kita Mularskog iz FBI-ja, inspektora Bilala Šena iz Odseka za borbu protiv krijumčarenja i organizovanog kriminala turske policije i detektiva Krisa Dosona iz policije Hambersajda. Sva trojica su se odrekla mnogo svog dragocenog vremena da bi vodila izuzetno prosvetljujuće razgovore sa mnom i nikad im nije bilo teško da mi objasne ono što nisam u potpunosti razumeo. Takođe, želim da zahvalim i agentima iz SOCA u Londonu i Kristijanu Agrumu, bivšem direktoru OCLCTIC-a u Parizu.

Iz sasvim drugačije perspektive, RioRita je u Ukrajini bio pravi rudnik informacija o CarderPlanetu i mnogo čemu drugom – na čemu sam mu posebno zahvalan. RedBrigade me je uputio u praktične pojedinosti sajber kriminala i mnogo mu dugujem zbog njegove srdačnosti i dobrodušne reakcije na moje bezbrojne zahteve za informacijama i analizama.

Matrix001 i JiLsi su uvek bili spremni da podele sa mnom ono što znaju o DarkMarketu i svoju procenu pojedinih događaja. Maks Vižn je bio briljantan i koristan sagovornik u Pitsburgu. Sva trojica imaju moju najiskreniju zahvalnost.

Čagataj Evjapan i Mert Ortač spadaju među najzanimljivije ličnosti koje sam upoznao u protekle tri godine, mada im se stavovi razlikuju. Želim da kažem koliko sam im obojici zahvalan, uprkos težini situacije u kojoj se trenutno nalaze.

U Estoniji, Madis Tur je bio uzoran vodič kroz istoriju i politiku te zemlje, kao i izuzetan i uvek zabavan domaćin.

Hvala i Bruksu Desiliji iz CBC-ja u Kalgariju na njegovom nesebičnom istraživanju, kao i Danijelu Goldbergu i Linusu Lašonu koji su mi pritekli u pomoć u Stokholmu.

Pozadinsku pomoć oko tehničkih pitanja pružila su mi dvojica ljudi – Miko Hiponen iz Helsinkija, glavni istraživač kompanije F-Secure, i Visente Dijaz iz Kasperski Labsa u Barseloni, kojima sam mogao da se obratim svaki put kad naiđem na nešto što jednostavno ne mogu da shvatim. Takođe, mnogo mudrih saveta u vezi s opštim pitanjima sajber bezbednosti dobio sam od Reksa Hjuza sa koledža Volfson, u Kembridžu.

Želim da izrazim svoju zahvalnost sledećim ljudima koji su mi na razne načine pomogli: to su Alison Kaliford, Luk Demboski, Sofi Devonšir, Joris Evers, detektiv Spenser Frizeli, Tamara Gleni, Kamino Kavana, Suat Kiniklioglu, Dirk Kolberg, Deril Lining, Melisa Levelin-Dejvis, Džejn Maklelan Q.C., Mark Mediš, Stiv Milner, Jan Prisalu, Kolin Robinson, Anja Štiglic i Eneken Tirk.

Moji agenti i izdavači bili su nepokolebljivi u svojoj podršci. Kler Konvil iz Londona je najbolji agent koga možete zamisliti, naravno, uz podršku divnog tima. Majkl Karlajl pruža podjednako dinamičnu uslugu u Njujorku. Srećan sam što imam urednički trojac koji sačinjavaju Vil Salkin u Bodley Headu, Den Frank u Knopfu i Sara Maklaklan u Anansi Pressu, koji su doprineli da mi sam period pisanja bude podnošljiviji i istovremeno umnogome poboljšali krajnji proizvod. Ako su se i potkrale neke greške, za njih sam, razume se, odgovoran isključivo ja. Želeo bih da zahvalim još dvema osobama koje su imale značajnog uticaja na ovu knjigu – Kej Pedl u Bodley Headu i Džejni Jun u Anansiju.

Moje troje dece, kojima je ovo delo posvećeno, sačuvali su zdravo interesovanje za knjigu i pored toga što sam često bio

fizički odsutan, ali i odsutan duhom u periodu dok sam pisao. Nikad nisu bili drugačiji do vedri i puni podrške.

Najzad, veliko hvala, uz mnogo ljubavi, Kirsti Lang, mojoj supruzi, koja je komentarisala, kritikovala, nežno ubeđivala i davala mi snage da nastavim. Po ko zna koji put, ne bih uspeo bez nje.

Jun 2011.

SADRŽAJ

7 Prolog

19 **KNJIGA PRVA**

Deo I

21 Inspektorov poziv
27 Miranda priča o hrabrom novom svetu
35 Gospodin Hajd iz Lagosa

43 **Deo II**

45 Dosijei Odesa
52 Carderplanet
54 Porodična stvar
63 Udavljeni udav
70 Iznova napisana skripta

75 **Deo III**

77 Tigar, tigar
81 Teorija igre
85 Nema povratka
90 Put u Indiju
93 Shadowlands

101 **Deo IV**

103 I dođe Iceman
107 Cardersmarket
112 DarkMarket

117 Kancelarija
125 Podozriva priroda
129 Doni Brasko
136 Lukavi plan

141 **Deo V**
143 Dronovo zaveštanje
148 Dečko, baš si ga uprskao
152 Udešena matrica
156 Francuska veza
161 Nevidljivi čovek

167 **Interludij**
169 Zemlja o kojoj ne znam ni šta ni gde

189 **KNJIGA DRUGA**
Deo I
191 Bilal u Pitsburgu
200 Visoka porta

205 **Deo II**
207 Ćao, ChaO
212 Nežno nežno nežnije

219 **Deo III**
221 Orijentacija
223 Svet mašte Merta Ortača
230 Sluga dvaju gospodara
235 Sladak život
240 Povratak u Had
245 Pohvatani na legalu

249 Smrt DarkMarketa

251 **Deo IV**
253 Ni kriv ni dužan
257 Zoro bez maske
263 Ko si ti?
264 Putovanje u nepoznato
268 Podnevni ekspres
273 Epilog
286 Napomena o izvorima
287 Reči priznanja